DIPLOMARBEIT

Titel der Diplomarbeit

A Fully Automated Quantum Cryptography System Based on Entanglement for Optical Fibre Networks

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag. rer.nat.)

Verfasser:	Alexander Treiber
Matrikel-Nummer:	0307368
Studienrichtung (lt. Studienblatt):	411
Betreuerin / Betreuer:	o.Univ.-Prof. Dr. DDr.h.c. Anton Zeilinger

Wien, am 24.08.2009

Contents

1. Abstract

This work presents the first compact, reliable and fully automated quantum key distribution (QKD) system based on entanglement[1]. The system is integrated into standard 19-inch cases and works at 1550nm for optimal use with optical fibres. Several newly developed automation and stabilisation modules like active adjustment of the entanglement source, polarisation control and detector synchronisation guarantee a reliable distribution of entangled photons.

The QKD system has been integrated into the European SECOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography) [2] quantum cryptography network which has been presented in October 2008 in the fibre network of Siemens Austria [3, 4]. During a two-week demonstration with an optical fibre of 16km length deployed between two locations of Siemens in Vienna, we could achieve an average entanglement visibility of 93% and a confidence level of 99.9% to have a visibility higher than 90%.

The high maturity level our QKD system allows us to deploy a practical quantum cryptography system almost on a plug&play basis. During the test phase over two weeks, a stable secure key rate above 2kbit/s with an average QBER of 3.5% was achieved without manual intervention. In the laboratory, a key exchange up to 50km with a key rate of more than 500bps is possible using commercial InGaAs detectors.

The results show that it is possible to distribute entangled photons reliably in an inner-city metropolitan area network (MAN) with standard telecom fibres under real world conditions despite several environmental fluctuations.

2. Introduction

In 2008, quantum cryptography made a large progress: the first quantum cryptography network with a flexible structure has been demonstrated. The quantum key distribution (QKD) system based on entanglement presented in this thesis was part of the European project SECOQC [2]. The quantum cryptography network has been presented in October 2008 in the fibre network of Siemens Vienna comprising six nodes and eight links.

Like every QKD system in the network, we had to fulfil several criteria:

- 19-inch compatibility: the complete QKD system has to be delivered in 19-inch cases to fit into standard 19-inch racks.
- Telecom wavelength: the photons travelling from Alice to Bob should have the standard telecom-wavelength (1550nm) to be compatible with standard single-mode fibres.
- Secure key rate at 25km: at least one kbit/second.
- Easy network integration: the devices should be able to be integrated to the network without manual adjustment of the optics inside.
- Reliable hands-off operation: the QKD system should reliably distribute keys between the nodes without any manual intervention for at least 24 hours.

This thesis presents an entanglement based QKD system that meets all above criteria. It is designed to work at 1550nm for the use in optical fibres and uses the entanglement based BBM92[5] key distribution protocol. The intrinsic correlations of an pair of entangled photons are used to extract a secure key that can be used for data encryption.

Up to now, entanglement has been an issue for quantum optics laboratories, quantum information theories and clearly not for reliable network devices that work on a hands-off basis. We are however confident that all modules presented within this thesis can be applied also to other entanglement-based quantum communication techniques for long term operation. We think, that even if entanglement-based QKD turns out to be not commercially viable (our system is indeed very close to a market-ready prototype), the automation and stabilisation techniques developed for this system will have impetus on the quantum communication community as a whole.

At the beginning of 2008, prototypes for polarisation and source stabilisation [6, 7, 8] existed with several remaining problems. Since crucial components like hands-off state alignment, detector (re-)synchronisation, system management and network integration were still not developed, the QKD system was far away from being ready for a hands-off long term operation.

Hence, the first part of this thesis was to develop automation and stabilisation modules that would bring the system to a mature hands-off level. A reliable distribution of entangled photons in a real-world environment (laid-out fibres, temperature fluctuations, etc.) was required. The second part was the integration of the system to the SECOQC network. A preview of the resulting QKD system is shown in fig. 2.1.

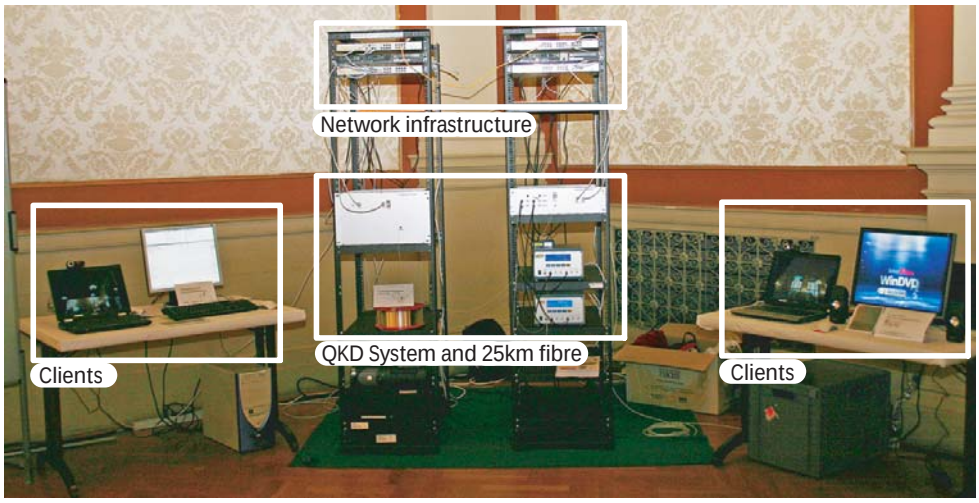

Figure 2.1.: The complete quantum cryptography system incorporating our entanglement based QKD system. The two 19-inch racks contain the QKD devices Alice and Bob that are connected using a 25km fibre spool. During a public demonstration, a live video conference between two clients has been encrypted using the link.

This thesis is structured as follows: Chapter 3 and 4 will give a short introduction to quantum information and quantum cryptography. Chapter 5 gives an overview of our QKD system. Chapter 6 presents the automation and stabilisation modules we have implemented to achieve the objectives. Chapter 7 presents several experimental results including the first long-term tests prior to the network integration. Chapter 8 will give a short overview of the SECOQC network in Vienna and explains the integration of our QKD system to the network structure. Finaly, the results during a two-week test phase are presented. To conclude, a short outlook on further developments of the QKD system and side-channel attacks is given in chapter 9. In appendix A, a new solution for real-time monitoring of the complete system and reliable database logging is presented.

3. Basics of Quantum Information

In the last decades, quantum communication and quantum information has matured from a purely fundamental research area to an applied science. Fundamental properties of quantum mechanics like superposition and entanglement give the qubit (the basic unit in quantum information) a completely new property and lead to several new applications like quantum cryptography, quantum teleportation and quantum computing.

At the moment, the most mature application of quantum communication is quantum cryptography [9, 10]. In the last ten years, quantum cryptography progressed from the first proof-of-concept experiments [11, 12] to prototypes for reliable and stable network devices like the system presented in this thesis.

This chapter will give a short overview of the basic elements in quantum information that are necessary to understand the principles of quantum cryptography.

3.1. The Qubit

The basic element of quantum information is the qubit. A qubit is a quantum-mechanical two-level system with two orthogonal states denoted as $|0\rangle$ and $|1\rangle$, analogous to the classical bit that can have the values 0 or 1. The two states $|0\rangle$ and $|1\rangle$ form an orthogonal basis in the two-dimensional Hilbert space. The striking difference to the classical bit is that the qubit can be in any superposition of the two basis states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{with} \quad |\alpha|^2 + |\beta|^2 = 1 \tag{3.1}$$

3.1.1. Polarisation encoded Qubits

In the QKD system presented in this work, qubits will be realised by the polarisation state of single photons. This has several advantages: photons can be transported in optical fibres, easily manipulated with optical elements and measured on a single photon level.

The qubit basis states are mapped to $|H\rangle$, a single photon with horizontal polarisation and $|V\rangle$, a single photon with vertical polarisation.

$$|0\rangle \longrightarrow |H\rangle \tag{3.2}$$
$$|1\rangle \longrightarrow |V\rangle \tag{3.3}$$

Throughout this work, some other distinct polarisation states and their qubit-representation will be used:

$$|P\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \quad +45^\circ \text{ linear} \tag{3.4}$$

$$|M\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \quad -45^\circ \text{ linear} \tag{3.5}$$

$$|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle) \quad \text{left-handed circular} \tag{3.6}$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle) \quad \text{right-handed circular} \tag{3.7}$$

3.1.2. Measuring a Qubit

Quantum mechanics only allows calculating the probability of measuring a qubit in a certain state. If one measures for instance the polarisation state $|P\rangle$ in the ($|H\rangle$, $|V\rangle$) basis, the probability is $|\alpha|^2 = 0.5$ to obtain horizontal polarisation and $|\beta|^2 = 0.5$ to obtain vertical polarisation. On the other hand, when the same state is measured in the P/M basis, the result will always be $+45^\circ$ polarisation. The state after the measurement is determined by the measurement value.

From this, another principle that is important for the security of quantum cryptography follows: in general, it is impossible to measure non-orthogonal states precisely and without perturbing these states. In other words, the state of a qubit can be determined with certainty only when the preparation basis is known.

3.1.3. No-cloning Theorem

A very essential property for the security of quantum cryptography is that a single qubit cannot be copied perfectly. This is known as the no-cloning theorem which was first shown by Wooters and Zurek [13]. A general cloning machine should copy the original qubit onto a blank qubit, i.e. should perform following operations:

$$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle \tag{3.8}$$

$$|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle \tag{3.9}$$

Where $|0\rangle|0\rangle$ denotes a two-qubit state. The first is the state to be cloned, the second is a blank target state that should hold the same state as the input afterwards.

If one chooses a superposition state, e.g. $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, then the machine will produce the following output due to the linearity of quantum mechanics:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \tag{3.10}$$

On the other hand, the output of the copying machine should be

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \quad &\longrightarrow \quad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \quad \frac{1}{2}\Big(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle\Big) \end{aligned} \tag{3.11}$$

which is clearly not the state 3.10. Generally, a universal cloning machine that copies an arbitrary initial state does not exist.

3.2. Entanglement

A pure two-qubit state that cannot be written as a product state $|\psi\rangle_{AB} = |\psi_A\rangle|\psi_B\rangle$ is called entangled. The definition sounds simple but implies a completely new quality. For example, consider the antisymmetric entangled state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\Big(|V_{A\rangle}|H_B\rangle - |H_A\rangle|V_B\rangle\Big) \tag{3.12}$$

The two individual qubits are in an undefined state while the overall state defines their joint properties. The state predicts strong correlations between the measurement results of the two qubits: although the measurement outcome is random, both qubits will always be found in an orthogonal state. Independent of the distance between the two qubits and of which part is measured first.

In quantum communication, the two systems sharing the entangled state are usually called Alice and Bob. When Alice measures the polarisation of her qubit, she will yield vertical or horizontal polarisation with a probability of 50%. Instantaneous, the post-measurement state becomes $|H\rangle|V\rangle$ or $|V\rangle|H\rangle$. Hence, Bob will measure vertical polarisation when Alice measured horizontal and vice versa.

State 3.17 is one of the four so-called Bell states that form a basis in the two-qubit space (four-dimensional Hilbert space):

$$|\psi^-\rangle = \tfrac{1}{\sqrt{2}}\Big(|H\rangle|V\rangle - |V\rangle|H\rangle\Big) \tag{3.13}$$

$$|\psi^+\rangle = \tfrac{1}{\sqrt{2}}\Big(|H\rangle|V\rangle + |V\rangle|H\rangle\Big) \tag{3.14}$$

$$|\phi^-\rangle = \tfrac{1}{\sqrt{2}}\Big(|H\rangle|H\rangle - |V\rangle|V\rangle\Big) \tag{3.15}$$

$$|\phi^+\rangle = \tfrac{1}{\sqrt{2}}\Big(|H\rangle|H\rangle + |V\rangle|V\rangle\Big) \tag{3.16}$$

The speciality of the $|\psi^-\rangle$ state is it's rotational symmetry. The state has the same form independent of the measurement basis:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle|V\rangle - |V\rangle|H\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|P\rangle|M\rangle - |M\rangle|P\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|R\rangle|L\rangle - |L\rangle|R\rangle\Big) \tag{3.17}$$

In contrast, the $|\psi^+\rangle$ state for example transforms to $|\phi^-\rangle$ in the P/M basis. Therefore, the $|\psi^-\rangle$ state is very applicable for the quantum cryptography protocols that will be presented in the next chapter.

3.2.1. EPR-Paradox and Bell-Inequalities

It is remarkable that entanglement can be used to solve a practical problem like data encryption but has it origins from fundamental questions concerning the completeness of quantum mechanics provoked by Einstein, Podolsky and Rosen (EPR-paradox) [14] in 1935.

EPR argued that a measurement on one side may not have an instantaneous (non-local) influence on the state of a arbitrary distant qubit. When Alice measures her part of the entangled state first, yielding randomly either vertical or horizontal polarisation when a $|\psi^-\rangle$ state is shared, Bob's qubit is left in a well-defined state. EPR argued that the quantum mechanical description cannot be considered complete since the definiteness of Bob's state is not part of the quantum mechanical formalism. In their opinion, the measurement result of both qubits should be explainable by a local realistic theory (e.g. a list of hidden parameters the photons carry along).

Almost 30 years later, John Bell showed in 1964 that no such local realistic theory can explain all predictions by quantum mechanics, in particular the correlations in an entangled state [15]. Bell derived an inequality for correlation measurements that should be obeyed by local realistic theories. However, the inequality has since then been violated in many entanglement experiments, e.g. [16].

4. (Quantum) Cryptography

Cryptography is the study of hiding information. In the last 2500 years, encrypting messages to keep information confidential has been primary a military issue. Nowadays - in the era of the information society - large parts of our daily routine are dominated by electronic communication: e-mail, telephony, e-banking, online-shopping, credit card payments, etc. Clearly, data security and cryptography has become an important issue for everyone. This chapter will give a short overview on classical and quantum approaches to cryptography.

In the usual scenario, Alice[1] wants to send a message to Bob in a way that no eavesdropper (Eve) can intercept the message. For this purpose, Alice and Bob use a cryptographic system. Most of the modern cryptosystems are based on publicly announced algorithms and standardized protocols, the security only depends on the secrecy of the keys [18][2]. Dependent on the usage of the keys one can distinguish two kinds of cryptosystems:

- A symmetric system uses the same key for sender (encryption) and receiver (decryption)
- An asymmetric system uses different keys for encryption and decryption

4.1. One-Time-Pad

Gilbert Vernam suggested to use a random bit-string as the key to encrypt a binary encoded message[19]. Later, this method got to be known as One-Time-Pad (OTP) because the key - written on a pad - should be used only once. Vernam's cryptosystem works as follows:

1. Alice applies a bitwise XOR on the message and the key. The result is the cipher text that is transmitted over the public channel
2. Bob applies a bitwise XOR on the cipher text and key to retrieve the message

This scheme is absolutely secure when four conditions are fulfilled:

1. The key is random (Eve has no information on the key and can only guess)
2. Alice and Bob have the same key (OTP is a symmetrical cryptosystem)
3. The key is exchanged secretly (only Alice and Bob know the key)

[1] Alice and Bob appeared for the first time in [17]
[2] This is known as Kerckhoff's principle

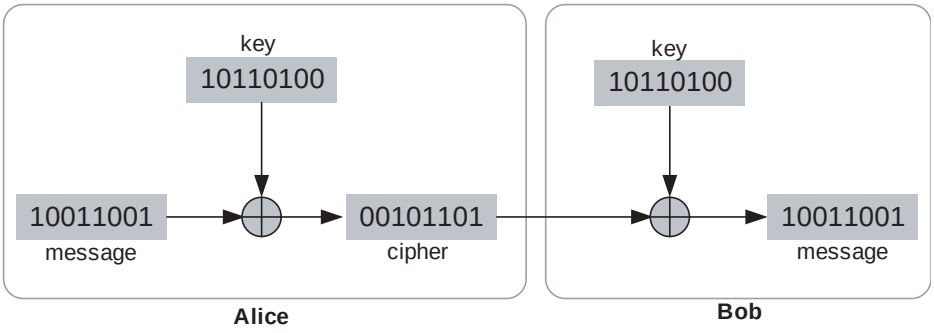

Figure 4.1.: One-Time-Pad scheme.

4. The key is only used once (by using the key more then once, the XOR scheme can be cracked immediately by looking for auto-correlations)

On the other hand, the OTP-scheme imposes several disadvantages:

- First, computer algorithms are not able to generate real random numbers, only so-called pseudo random numbers.
- More important is the practical disadvantage of OTP that the key needs to have the same length as the message. It is therefore not applicable for typical internet communication and even less for practical data networks (LAN, WAN).

To overcome this drawback, modern symmetrical cryptosystems like the current standard AES (Advanced Encryption Standard) use the same key to encrypt more than one message (block ciphers). The key is usually distributed prior to data transmission and should be refreshed frequently[3]. At the moment, it is assumed [18] that a renewal rate of one minute is more than sufficient even for the fastest available AES encryption. AES is considered secure and practically useful but has the same problem as OTP: how can one distribute a key between Alice and Bob securely? This is known as the key distribution problem.

4.1.1. Key distribution: classical approach

In 1975, Whitfield Diffie and Martin Hellman [20] suggested to use a mathematical one-way function for an asymmetric cryptosystem. The Diffie-Hellman key-exchange is based on modulo-operations and allows Alice and Bob to establish a key without exchanging the actual key.

Two years later, in 1977, Rivest, Shamir and Adlemen (RSA) found a similar algorithm to encrypt and decrypt messages without prior distribution of a secret key. The RSA cryptosystem, which is employed by all common internet-protocols (SSL, TLS) uses two different keys:

- The public key is used for encryption and is announced publicly
- The private key is used to decrypt the message and has to be kept secret

[3] Internet protocols like SSL/TLS exchange the session key only once, e.g. when the users enters the https-website

The security of the system lies in the difficulty of factoring large numbers and hence is based on assumptions of computational power of practical computers. In 2003 Shamir (the S in RSA) and Tromer suggested a hardware design [21] that is able to crack an RSA 1024 key (to extract the private key out of the public key) within one year at a total cost of 10-50 million dollars. 1024 is the typical key length used nowadays for most applications. In 2007, a group at the University of Bonn succeeded to factorise a 1039-bit number [22]. Because of the possibility to parallelise the factoring algorithms, computational power is not a matter of technologies but a financial issue. Furthermore, there is no proof that no efficient algorithm exists which could then crack RSA more efficiently. Although not feasible at the moment, a quantum computer poses another threat to classical cryptography. Peter Shor showed that a quantum algorithm exists that can solve the factoring problem efficiently [23].

4.2. Quantum Key Distribution (QKD)

Although the idea to use quantum mechanics for encryption was first proposed by Stephen Wiesner in the 1970s [24], the first practical protocol was developed by Charles Bennett and Gilles Brassard in 1984 [25]. In their scheme, the laws of quantum information are used to distribute a key secretly. As pointed out earlier, it is the security of the key that makes a cryptosystem secure.

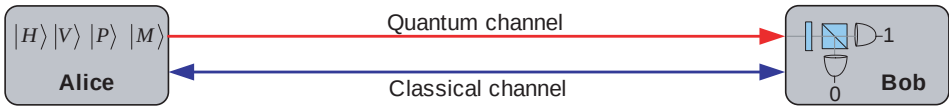

Figure 4.2.: Scheme for the BB84 protocol: Alice and Bob are connected by a quantum channel (unidirectional) and a public classical channel

In the BB84 scheme, Alice and Bob are connected by two channels: a quantum channel and a classical channel which does not need to be secure, but authenticated.

1. Alice chooses randomly one of four non-orthogonal polarisation states $|V\rangle$, $|H\rangle$, $|P\rangle$, $|M\rangle$ and sends a single photon prepared in that state to Bob using the quantum channel.
2. Bob measures the photon's polarisation by randomly choosing the H/V or P/M basis

Afterwards, the polarisation state prepared by Alice and measured by Bob is assigned to a classical bit:

$$\begin{aligned} |H\rangle &\longrightarrow 0 \\ |V\rangle &\longrightarrow 1 \\ |P\rangle &\longrightarrow 0 \\ |M\rangle &\longrightarrow 1 \end{aligned} \tag{4.1}$$

Alice and Bob continue this scheme to obtain a correlated bit-stream with a given length, the

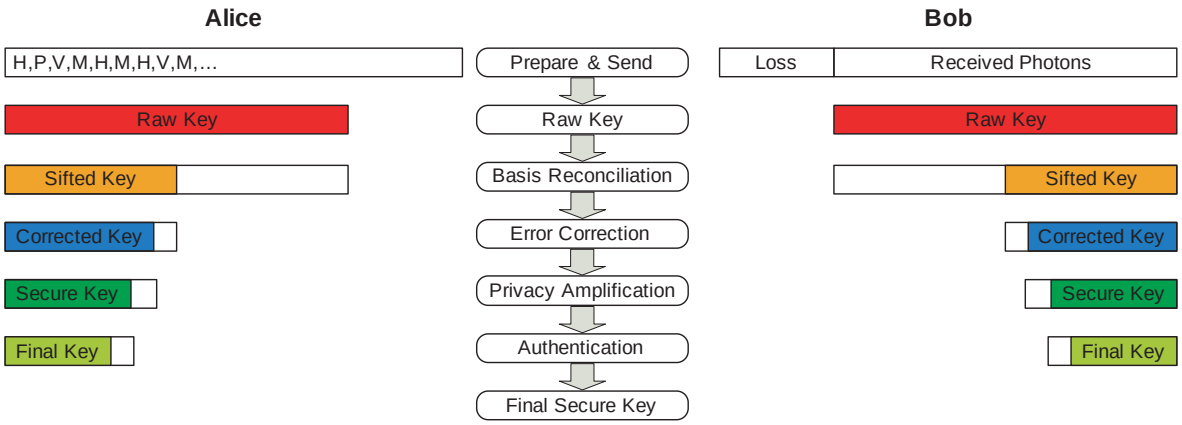

Figure 4.3.: QKD protocol stack: Alice first prepares and sends a sequence of polarisation encoded qubits. The raw bit string (raw key) that Alice and Bob share after the measurements is then reduced in several steps to obtain a secure and error-free key.

so-called raw key (an example is given in table 4.1). To extract a secure key from the raw key, some more steps are necessary (figure 4.3).

	Alice		Bob		
Number	Sending	Key-Bit	Basis	Result	Key-Bit
1	H	0	H/V	H	0
2	V	1	P/M	?	?
3	P	0	H/V	?	?
4	M	1	P/M	M	1
5	V	1	H/V	V	1
6	P	0	P/M	P	0
7	M	1	H/V	?	?
8	H	1	P/M	?	?

Table 4.1.: Example for the BB84 quantum key distribution (QKD) protocol. Alice sends a random sequence of qubits, here polarisation encoded photons. Bob randomly chooses the measurement basis. A '?' represents the case when Alice and Bob used different basis and Bob will obtain a random result. These bits will be discarded later by the basis reconciliation procedure.

The security of this scheme lies in the use of two non-orthogonal bases. A potential eavesdropper (Eve) does not know the basis. As mentioned in the previous chapter, a measurement principally changes a quantum state that is not orthogonal to the measurement basis. Therefore every interaction with the single photon will unavoidably introduce some errors. Eve could simply try to measure the photon and resend the obtained state. Since Eve does not know the basis, she must guess and hence introduce errors with a probability of 25%. By comparing a fraction of the key, Alice and Bob can immediately detect Eve's activities by looking on the number of errors in the key. A compromised key will be discarded immediately.

4.2.1. Basis reconciliation

Alice and Bob will only share the same state when Bob measures in the basis of the transmitted photon. As Eve, also Bob does not know the basis Alice used. For example, when Alice sends a qubit in state $|H\rangle$ and Bob chooses the P/M basis, he will randomly obtain either P or M (each with a probability of 50%). Therefore, Bob uses the classical channel to tell Alice which basis he used after the measurement. Subsequently, Alice and Bob discard their entries in which they used different basis. The output is called the sifted key and has approximately half the length of the raw key. Note that the classical communication used for the sifting process only contains the measurement basis and not the measurement result (classical bit value).

4.2.2. Error Correction

In a real QKD system, some unavoidable errors will be introduced even when no eavesdropping occurs. Analogous to the classical bit error ratio (BER), the qubit error ratio (QBER) is defined as the ratio of wrong bits to the total number of bits in the sifted key. The inherent wrong bits can be corrected using classical protocols.

The minimum number of bits r_{opt} that needs to be exchanged between Alice and Bob for error correction is given by Shannon's coding theorem [26]

$$r_{opt} = n_{sifted} \cdot h(e) \tag{4.2}$$

where n_{sifted} is the length of the sifted key and e the QBER with Shannon's binary entropy function[4]

$$h(e) = -e\, log_2(e) - (1-e)\, log_2(1-e) \tag{4.3}$$

However, it is not possible to reach this limit. Realistic error correction protocols need to exchange more bits to locate the errors. The algorithm used in our QKD system - CASCADE [27]- is based on intense bidirectional communication of parity bits (on the public channel). As figure 4.4 shows, CASCADE works about 15% to 21% above the Shannon limit.

$$r_{real} = f(e) \cdot r_{opt}(e) \qquad \text{with} \qquad f(e) \geq 1 \tag{4.4}$$

Eve could use the information leakage during error correction to obtain some knowledge of the key. Therefore, the key needs to be shortened by the number of bits exchanged (r_{real}) using an error-dependent hash-function. The implementation of the error-correction process in our system also allows to estimate the QBER in the overall key. Hence it is not necessary to compare a fraction of the key over the classical channel.

4.2.3. Privacy Amplification

Using various attack strategies, Eve can obtain information about the key. Generally, every attempt by Eve to increase her knowledge of the key will also increase the QBER. The privacy

[4] $h(e)$ is the conditional entropy for a binary symmetric channel with a bit-inversion probability e

amplification [28] technique allows reducing Eve's knowledge to a minimum. For this purpose, an error-dependent hash-function is used to map the input-string to a shorter output string

In [29] Norbert Luetkenhaus gives a bound for the maximum amount of information in bits Eve can have for a certain QBER.

$$\tau(e) = \begin{cases} log_2(1 + 4e - 4e^2) & \text{for } e < 0.5 \\ 1 & \text{for } e \geq 0.5 \end{cases} \tag{4.5}$$

$\tau(e)$ determines the length of the error-dependent fraction by which the key has to be shortened during privacy amplification. Note that equation 4.5 is valid only for individual attacks where Eve accesses only one photon at a time. For more general attack schemes (where Eve can access more than one photon coherently) the number of bits to be discarded is equal to Shannon's entropy $h(e)$ [30, 31].

Combining error correction and privacy amplification gives the length of the resulting secure key (n_{sifted} is the size of the sifted key):

$$\begin{aligned} n_{secure} &= n_{sifted}\,[1 - \tau(e)] - r_{real}(e) \\ &= n_{sifted}\,[1 - \tau(e) - f(e) \cdot h(e)] \end{aligned} \tag{4.6}$$

In our system, the security-related key-reduction for privacy amplification and error correction is done in one step using a Toeplitz-Matrix with the size $n_{secure} \times n_{sifted}$. Figure 4.4 shows that is possible to obtain a secret key up to a QBER of 11.4% for ideal error correction and 9.7% when the CASCADE protocol is used.

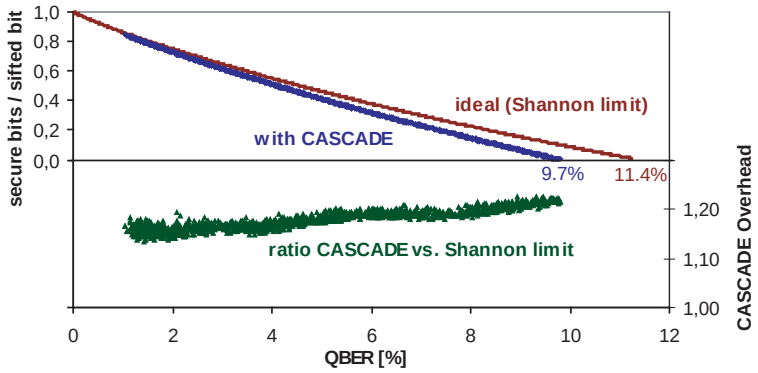

Figure 4.4.: Top: number of secure bits per sifted bit in the case of ideal error correction compared to the CASCADE error correction protocol. Note that the blue line originates from our experimental values.
Bottom: Overhead $f(e)$ of the CASCADE error correction protocol compared to the ideal error correction (Shannon limit). CASCADE works about 15% to 21% above the Shannon limit. The "cloudy" shape of the overhead function comes from the heuristic approach of CASCADE. The actual number of exchanged bits depends on the distribution of wrong bits in the key and thus can vary for keys with the same QBER.

Privacy amplification allows to deal with (theoretical) attacks on the BB84 protocol, i.e. directly on the qubits. A completely different and technically feasible approach is to attack the

implementation of the protocol and not the protocol itself. Such attacks are called side-channel attacks and pose a realistic threat to every QKD system. Section 9.4 will give an overview of the implications of several side-channel-attacks on our QKD system.

4.2.4. Authentication

The privacy amplification technique described above cannot rule out a so-called man-in-the-middle attack where an intruder tries to control the communication between Alice and Bob.

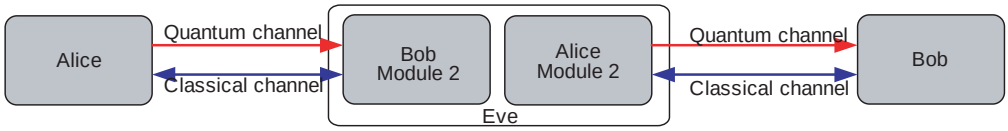

Figure 4.5.: "Woman-in-the-middle" attack: Eve cuts both channels and pretends to be Alice and Bob

This is not a completely unrealistic scenario because Eve could simply buy the devices from the reseller (e.g. from idQuantique [32] when she knows that the QKD-link is provided by this company) and cut both channels. Therefore, Alice and Bob have to ensure that their vis-á -vis is really the one they want to communicate with.

For this purpose, a classical authentication method proposed by Wegman and Carter in 1981 [33] can be used (figure 4.6). Before the QKD system is installed, a pre-shared authentication-key is set in the factory (or laboratory). When the first key-block leaves the QKD protocol stack, an authentication tag is calculated from the key-block using a hash-function that depends on the authentication-key. For authentication, Alice and Bob subsequently compare the tag. The tags calculated by Alice and Bob are equal if and only if both used the same pre-shared authentication-key.

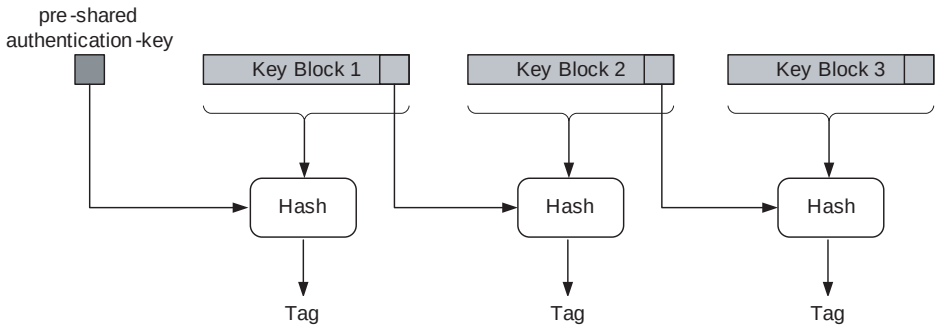

Figure 4.6.: Authentication scheme to prevent man-in-the-middle attacks.

To authenticate the next key-block, a fraction of the previous key block is kept as the next authentication-key. The BB84 protocol is therefore sometimes denoted as a Quantum Key Growing protocol since a initial pre-shared key is required.

4.2.5. Data encryption

QKD only deals with the secret distribution of keys between Alice and Bob. For data encryption, classical algorithms like one-time-pad (OTP) or AES are used.

4.3. Entanglement based QKD

In 1991, Artur Ekert proposed a protocol that is based on entanglement [34]. A source creates entangled qubits and distributes them to Alice and Bob. The correlations of a shared entangled state can be used to yield a symmetric key. In the original scheme, Alice and Bob use a fraction of the raw key to check a Bell-inequality. If it is violated, then no eavesdropper was active. If Eve tries to intercept and resend the photons, she acts as a deterministic photon source and therefore leads to a valid Bell inequality.

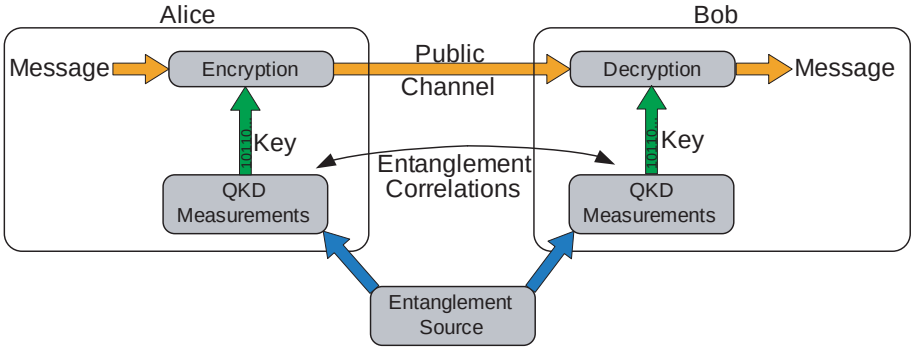

Figure 4.7.: Scheme for entanglement based quantum cryptography. A source distributes entangled photons between Alice and Bob where the entanglement correlations are used to establish a secure key. For practical purposes, the entanglement source also can be integrated in one of the QKD devices.

One year later, Bennett, Brassard and David Mermin [5] modified the original BB84 protocol and added an entanglement source that distributes the photons to Alice and Bob. This is the protocol we use for our QKD system. The difference to the BB84 protocol is that both Alice and Bob randomly choose either the H/V or the P/M basis and measure the polarisation of an shared entangled state. When Alice and Bob share the $|\psi^-\rangle$ state, they will obtain random but perfectly correlated measurement results when both used the same measurement basis (Bob has to reverse his bit string since $|\psi^-\rangle$ predicts anti-correlated results). This already meets two of the requirements for an absolutely secure OTP cryptosystem (a random but equal key string on both sides). Basis reconciliation and the other parts of the BB84 protocol do not need to be modified.

Compared to the BB84 protocol (prepare-and-measure), BBM92 has a significant advantage: no external random number generator or any other active component which can be compromised is necessary. As shown in the next chapter, the protocol can be implemented using passive components only.

5. Overview of the QKD System

This chapter gives an overview of the components of the whole QKD system (fig. 5.1). The complete setup consists of the following:

- two 19-inch cases: Alice and Bob
- a quantum channel (single-mode fibre) connecting Alice and Bob
- two computers for the BBM92 post-measurement protocol (sifting, error-correction, authentication)
- a classical channel connecting the computers

5.1. Alice

The core of the system is the polarisation-entangled photon source emitting pairs with asymmetric wavelengths (810nm and 1550nm). Details of the source can be found in [35]. Here it is sufficient to say that a 532nm cw-laser pumps two ppKTP crystals for type-I spontaneous parametric downconversion (SPDC). The two crystals are poled for collinear emission of 810nm and 1550nm photons. The polarisation state after the two crystals is given by:

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_{810}|H\rangle_{1550} + e^{i\phi}|V\rangle_{810}|V\rangle_{1550}) \tag{5.1}$$

The 810nm and 1550nm photons are split using a dichroic mirror and coupled into single mode optical fibres. For an active stabilisation of the entanglement source (see sec. 6.1), the fibre couplers and a mirror after the laser are assembled on piezo mounts with two tilt axes.

The 810nm photons pass an in-fibre polarisation controller before entering the BB84 module. Here the photons are recollimated onto a balanced beamsplitter (BS) and then directed to two polarising cube beamsplitters (PBS). The PBSs are rotated by 45°relative to each other along the transmission axis to perform measurements in the 0°/90°(H/V) and in the +45°/-45°(P/M) basis.

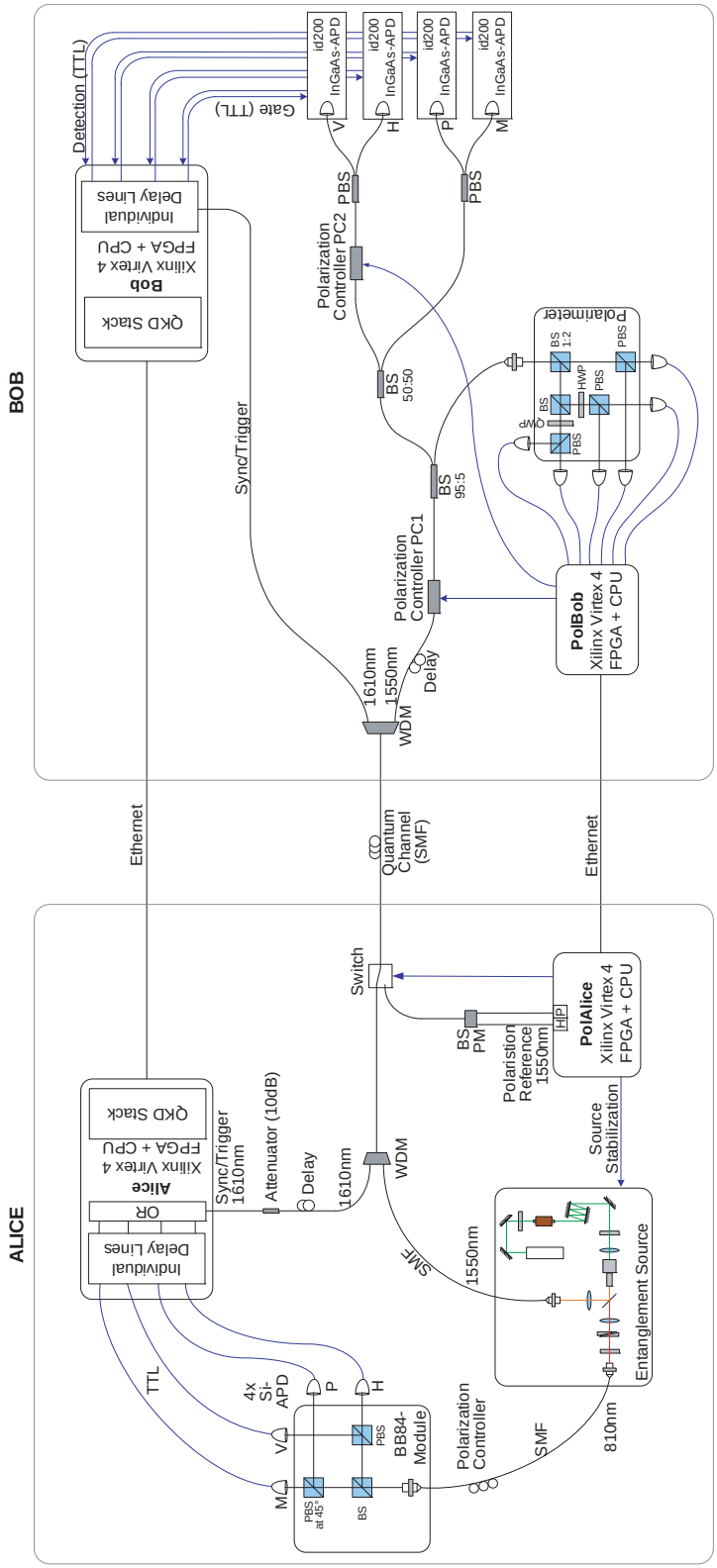

Figure 5.1.: Overview of the complete QKD system

The four output ports of the PBSs are coupled into multimode fibers connected to an array of four Si-APDs (SPCM-AQ4C from Perkin Elmer). The TTL outputs from the detectors are fed into an electronic board (Xilinx Virtex 4 FX20). All FPGA boards used in the system (Alice, Bob, PolAlice, PolBob) are combinations of a Xilinx Virtex 4 platform providing the FPGA logic and embedded CPU (IBM PPC405) together with custom-built electronics.

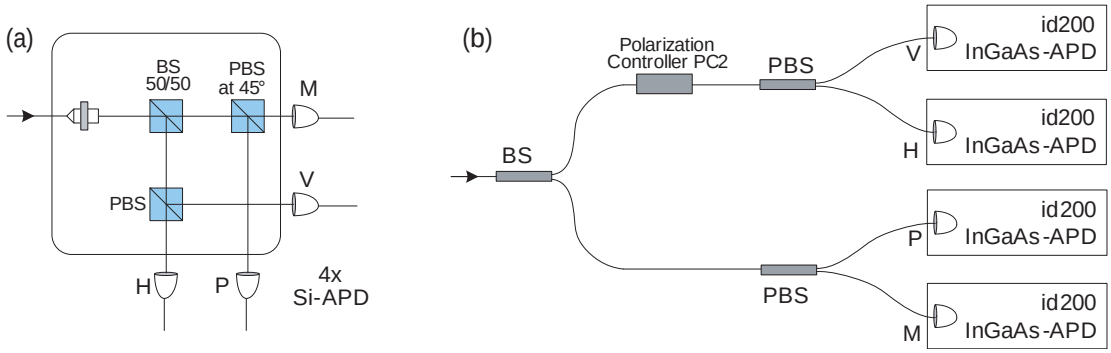

Figure 5.2.: (a) free-space BB84 module for Alice. The 50/50 beam splitter randomly transmits or reflects a single photon and hence carries out the random selection of the measurement basis. The polarising beam splitter (PBS) transmits a horizontal photon and reflects a vertical photon. The second PBS is rotated 45°in respect to the other to perform the measurement in the P/M basis.
(b) all-fibre BB84 module for Bob. The polarisation controller allows to rotate the measurement basis of the first PBS to 45°in respect to the second PBS.

Every time a 810nm photon is detected at Alice, a strong synchronisation pulse at 1610nm is generated and merged with the single photons at 1550nm using a WDM (wavelength division multiplexer). Before sending the sync-pulse, the detection event is delayed individually for every channel to prevent side-channel attacks (see sec. 9.4.2). The pulse at 1610nm is used to synchronise the detection events between Alice and Bob and to trigger Bob's InGaAs-detectors.

After the WDM, the signals pass an optical switch necessary for the operation of the polarisation stabilisation. The fibre is connected at the front plate of Alice to the quantum channel (a standard telecom single-mode fibre, SMF), allowing the 1550nm photons to travel to Bob. The second input to the optical switch comes from PolAlice, another Xilinx board that is used for stabilisation purposes. PolAlice drives the piezo mounts for source stabilisation (see sec. 6.1) and two laser diodes at 1550nm for polarisation control (see sec. 6.3).

The quantum channel is multiplexed in time and wavelength (fig. 5.3). During the QKD operation, the sync-pulse (1610nm) follows the single photon (1550nm). For polarisation control purposes, the quantum channel is switched to PolAlice sending reference pulses with certain polarisation (H and P) at 1550nm.

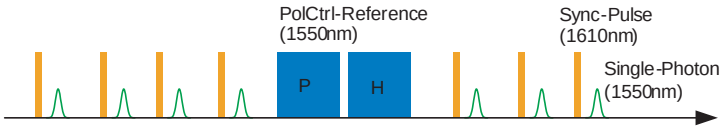

Figure 5.3.: Timing-sequence of single photons, sync-pulses and polarisation control (PolCtrl) reference pulses showing the time and wavelength multiplexing of the quantum channel.

5.2. Bob

On Bob's side, almost all optical components are fibre based. First, a WDM-demultiplexer splits the sync-pulses at 1610nm from the 1550nm channel (single-photons and reference pulses for polarisation control).

The 1610nm sync-pulse is converted to an electronic signal at a FPGA electronic board. After an individual delay for precise detector synchronisation (see sec. 6.4), a trigger pulse (TTL) is passed to the InGaAs detectors where the gate voltage is applied just at time when the photon is expected.

The single photons at 1550nm first pass a 32m delay fibre to give the InGaAs detectors time to apply their gates. Subsequently, the single photons pass an electronic polarisation controller (General Photonics PolaRite II [36]) and an unbalanced 95:5 beam splitter to reach the fibre-based BB84 module. One arm of the BB84 module contains another polarisation controller to rotate the measurement axis of the first basis (H/V) to 45°with respect to the other basis (P/M). All four outputs of the two PBSs are coupled to InGaAs APDs (IdQuantique id200/id201).

A small fraction (5%) of the 1550nm light is coupled out before the BB84 module and is directed to a classical six-channel polarimeter where the strong reference pulses from PolAlice are analysed. The polarimeter and the PolaRite controller in the quantum channel are used for polarisation control purposes (see sec. 6.3).

The sync-pulses at 1610nm also facilitate the synchronisation of detection events needed for the sifting process. Before sifting, Bob tells Alice which trigger pulses resulted in a detection event. Alice deletes all other entries. Both share subsequently a raw key of the same length that is processed by the QKD protocol stack (see sec. 4.2) to yield a secure key.

The software implementing the QKD protocol stack is located on two computers that are connected to Alice and Bob via Ethernet. Alternatively, the QKD stack can run directly on the embedded CPU (PowerPC 405 for a single-chip solution ("Quantum Cryptography on a Chip" [37]). However this approach is limited to key rates of about 1kbit/s due to computational limitations of the embedded CPU.

5.3. 19-inch packaging

The system was designed to be installed in a standard 19-inch rack. Therefore also all components have to fit into 19-inch cases.

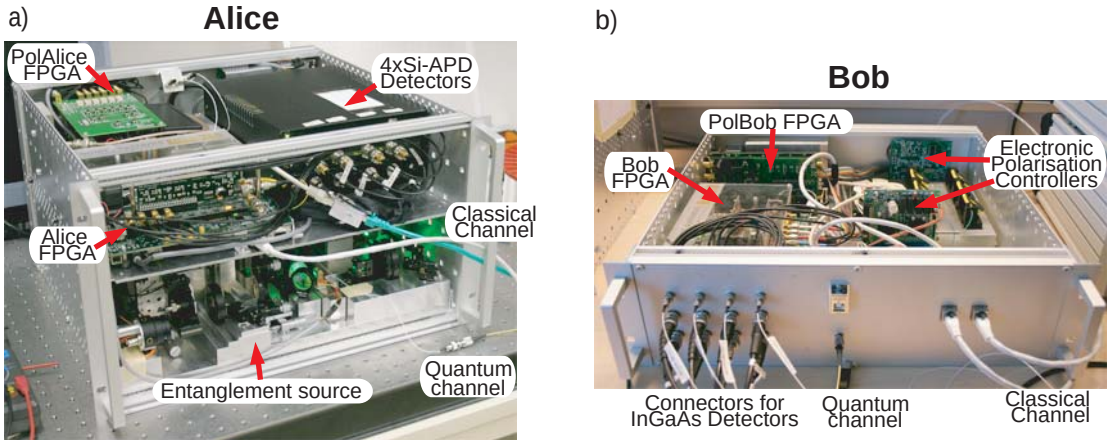

Figure 5.4.: Alice (6 height units, approx. 26cm) and Bob (3 HU, approx. 13cm) in their final 19-inch cases. Only the four InGaAs detectors at Bob need to be placed outside.

The entanglement source is assembled on a monolithic aluminium plate (42x26cm). It is located on the bottom in Alice's case, together with the BB84 module and the fibre switch. On top are the Si-detectors, the main power supply and the two FPGA boards (Alice, PolAlice). The front plate contains two Ethernet connectors for Alice and PolAlice, a JTAG interface for programming PolAlice and the fibre output for the quantum channel.

Bob's case contains the two polarisation controllers, the polarimeter (just behind the front side, not visible in fig. 5.4), the FPGA boards (Bob, PolBob) and the fibre based BB84 module which is encased in plastic. Only the four commercial InGaAs detectors do not fit into the case and need to be placed outside. They are connected using BNC cables for trigger and detection output and a short fibre for the single photons. The front plate contains two Ethernet connectors for Alice and PolAlice, a JTAG interface for programming PolBob, the interfaces to the detectors and the fibre intput for the quantum channel.

6. Automation and Stabilisation Modules

One of the main parts of this thesis deals with the automation and stabilisation of the complete QKD system to meet the requirements mentioned in the introduction. Three issues need to be considered: automation, stabilisation and coordination.

First, every task that is necessary to start the QKD system and is manually done in the laboratory has to be automated. In particular:

- Adjustment of the fibre couplers in the entanglement source to keep the entanglement rates high
- Adjustment of Bob's measurement axis to align the desired entangled state ($|\psi^-\rangle$)
- Precise synchronisation of the InGaAs detector gates with the arrival of the single photons

The second issue is the stabilisation of the QKD system once it is started:

- Active stabilisation of the fibre couplers in the entanglement source
- Stabilisation of the polarisation in the quantum channel
- Periodic detector re-synchronisation

The third issue is the coordination of the QKD system:

- Coordination of all modules for a hands-off start-up of the complete system.
- Coordination of the stabilisation modules during normal operation.
- Handling of errors that might occur during a long-term QKD run.

All these issues will be covered in the following sections. Note that none of these issues is QKD specific. One can consider the BBM92 protocol as an application that uses the entanglement correlations. As already mentioned in the introduction, we are confident these modules is can be applied also to other entanglement-based protocols that are currently on an experimental proof-of-principle level.

6.1. Source Stabilisation (SourceStab)

The entanglement source is based on free space optics and hence prone to mechanical drifts due to temperature fluctuations. The most crucial parts are the couplers where the single photons are coupled into single-mode fibres. Even small deviations from the optimal coupler position will reduce the coupling efficiency significantly. The focus of the pump laser is also important, deviations here (beam wander) will reduce the production rate of entangled photons

A reliable and fully automated stabilisation of the entanglement source is therefore absolutely inevitable to achieve a complete hands-off operation of the whole system. During the SECOQC demonstration, the source will be enclosed in a 19" case and is therefore not even accessible for manual control.

For this purpose, both couplers and a mirror behind the laser are assembled on piezo mounts AM-M100 from Newport with two tilt axes. All six piezo channels are driven by PolAlice. Unfortunately, the manufacturer does not provide any suitable (microprocessor-compatible) interface to the piezo actuators, only a remote (hand-held) control is provided. The FPGA therefore has to short-circuit the buttons of the remote control to make them accessible for the software running on the CPU. Additionally, the output of a single remote control is multiplexed using relays to access all six channels.

It is intuitively clear that the order of driving the piezo-actuators must be the same as the order of the optical elements in the source itself. The adjustment of the pump laser influences the production rate of photon pairs and hence influences the count rate on Alice and the coincidence rate on Bob. The coupling efficiency of the 810nm coupler influences the count rate on Alice witch is equal to the trigger rate of Bob's detectors. Therefore, the sequence of driving the piezo-mounts is:

1. Pump laser mirror
2. 810nm coupler
3. 1550nm coupler

Step 1 and 2 are based on Alice's count rate, Step 3 on Bob's coincidence rate. Alice and Bob therefore send their individual detector rates via Ethernet (UDP) in an one-second interval to PolAlice. The software running on PolAlice analyses the input (table 6.1) and drives the piezo-motors using a certain algorithm (Hill-Climber) to maximise the count rates.

Channel	Piezo-Component	Data source
0	Laser mirror, axis 1	Alice
1	Laser mirror, axis 2	Alice
2	810nm coupler, axis 1	Alice
3	810nm coupler, axis 2	Alice
4	1550nm coupler, axis 1	Bob
5	1550nm coupler, axis 2	Bob

Table 6.1.: Summary of the SourceStab channels and the data source (count rates) used for adjusting the piezo actuator

6.1.1. The Hill Climber Algorithm

The Hill Climber algorithm is a very simple heuristic algorithm for searching a local maximum. It is sketched in fig. 6.1 This algorithm can be easily adapted to our problems[1] and seems to be very suitable to solve them. The procedure starts by moving the piezo motor in one direction (up). The count rate can follow this change in two ways as shown in fig. 6.1. The SourceStab software running on PolAlice will apply this simple method consecutively to all six channels in the order mentioned earlier.

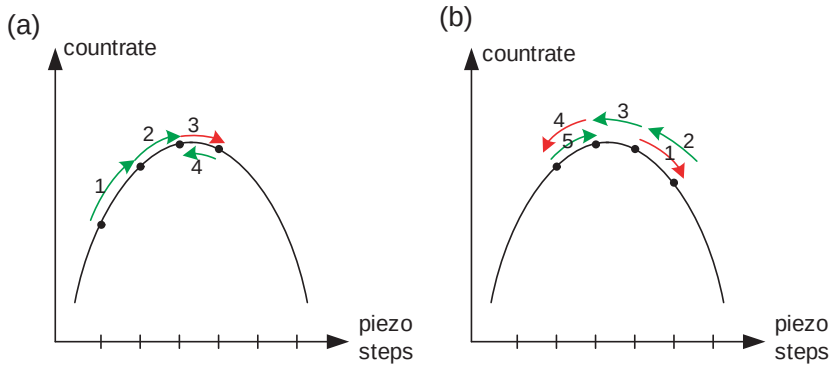

Figure 6.1.: Principle scheme of the Hill-Climber algorithm
(a) The first step leads to a higher count rate. Since it is the objection to maximise the count rate, the coupler will continue to move toward this direction (step 2) until the count rate is lower than the last step (3). If this happens, the motor goes back one step (4) to get as close as possible to the maximum.
(b) If the first step turns out to be in wrong direction (leads to lower count rates), the procedure immediately changes the direction until a maximum is found as in case A (steps 2-5).

[1] The same algorithm is also used to align the entangled state (sec. 6.2) and for detector resynchronisation (sec. 6.4.3).

For a reliable operation of SourceStab, some additional issues have to be addressed:

- When SourceStab is started, it is assumed that the count rates are not too far away from the maximum. Any automated version will not work if the count rates are at noise level (background counts). Therefore, the couplers need to be roughly aligned manually once, before the source is placed in the final 19" housing.
- Since we have to rely on single-photon count rates, a long averaging time is necessary. 10 seconds turned out to be useful.
- The algorithm will not find the exact position of the maximum. By reducing the step-size and running SourceStab periodically, the count rate is however locked very close to the maximum (within the typical short-term fluctuation of the count rate).
- The whole SourceStab procedure can run without interruption of the QKD process. In fact, it is the objective of SourceStab to keep the deviations of the count rates and therefore the influences on the key rate as small as possible
- During normal operation, the step-size is chosen to 2 piezo-steps (0.4 arc-s). During the system start-up, the step-size is 6 piezo-steps to retrieve larger deviations faster (e.g. after transport or long idle time).

6.1.2. Performance Tests

The final question of course is: Does SourceStab now work as it should and is it reliable?

For the first functional test of SourceStab, we applied manual deviations in an arbitrary direction on every channel using the piezo remote control. From figure 6.2 one can see, that SourceStab manages to retrieve the previous count rate perfectly. In the same manner, SourceStab succeeds to retrieve the count rate even after transporting the whole QKD setup (see fig. 6.17).

The most important point of course is the long-term stability of the count rates. Figure 6.3 shows the sum of Alice's count rates during a 100h test prior to the SECOQC demonstration. One can see clearly that SourceStab managed to keep the count rates stable. The small remaining fluctuations are due to fluctuations of the crystal temperature controller that affects the production rate of entangled photons.

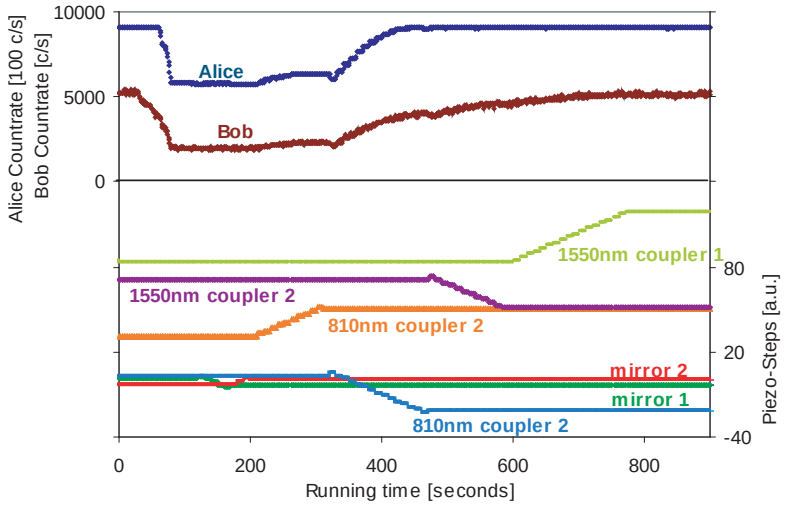

Figure 6.2.: SourceStab under test: at the beginning all six channels have been changed manually to decrease the count rates. On the lower half, one can see the steps of the piezo-mounts driven by PolAlice to retrieve the original count rates.

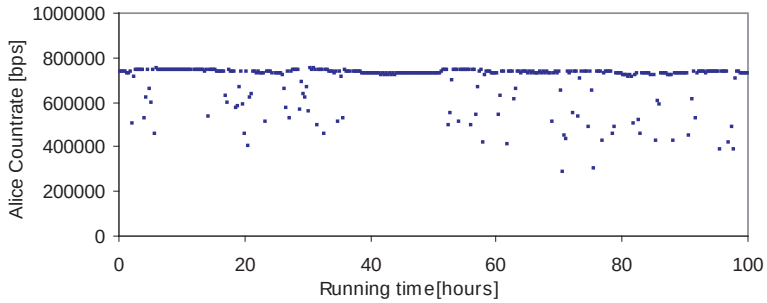

Figure 6.3.: Alice's count rate (sum of all four detectors) during a 100h test. The points below the average count rate derive from start-up and alignment processes. Bob's rates are not added to the chart because of problems with the long-term stability of the InGaAs-detectors that will be discussed later (see section 8.4.1).

6.2. Automatic Alignment of the Entangled State (StateAlign)

The unavoidable random distribution of birefringence in the fibre (quantum channel) will cause arbitrary unitary transformation of the single photon's polarisation state. For certain distances (as long as depolarising effects are negligible[2]) the induced transformation is unitary and hence can be completely compensated using polarisation controllers. For a polarisation coded QKD scheme, precise alignment of the polarisation entangled state is a crucial part.

In our case, the objective is to align a certain maximal entangled Bell-state between Alice and Bob[3]:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|V\rangle_A|H\rangle_B - |H\rangle_A|V\rangle_B) \tag{6.1}$$

This entangled state predicts a strong correlation between Alice and Bob: whenever Alice measures a vertical photon (with a probability of 50%), then Bob will measure a horizontal photon with certainty. When Alice measures horizontal polarisation, Bob will measure vertical polarisation.

To align this state precisely, we make use of the fundamental properties of the state itself. The probability of measuring both entangled photons in parallel polarisation is (ideally) zero. Furthermore, this is the only Bell state that is completely rotational symmetric, i.e. it has the same correlations in every basis. This allows to use the same method to align both bases (H/V and P/M) that are required for the BBM92 protocol. Since there is no classical equivalent to entangled quantum states, there is also no classical auxiliary aid like a reference pulse to align the entangled state. The only way is to use the coincidences itself.

6.2.1. Manual state alignment

The target state 6.1 is aligned in the H/V basis when the polarisation after the quantum channel is transformed in a way that coincidence rate on the V-detector is (ideally) zero when Alice triggers [4] only after measuring a vertical photon. In a scenario with realistic detectors, the minimum coincidence rate is not zero but given by the number of dark counts and accidental coincidences. After aligning the H/V basis, the same needs to be done for the P/M basis.

In the laboratory prototype of the QKD system, two manual polarisation controllers (so-called "bat-ears", see fig. 6.4) were used on Bob's side to align the entangled state. These consist of three fibre loops that can be turned with respect to each other and rotate the polarisation state in any direction.

[2] see for example [7] for an overview of depolarising effects in fibres
[3] all postmeasurement analysis on the FPGAs Alice and Bob is prepared for the $|\Psi^-\rangle$ state
[4] here, triggering means that Alice sends a sync-pulse

The procedure for the manual alignment looks as follows:

1. Unplug all Si-APD detector outputs except channel 0 (V-detector). This will cause Alice to send trigger pulses only when vertical photons are measured[5].
2. Minimise the coincidence rate on the corresponding single-photon detector at Bob (channel 0 - vertical) using the bat-ears of the H/V-base. As mentioned above this will align the entangled state in the H/V base.
3. Unplug all detector outputs except channel 2 (+45°detector).
4. Minimise the coincidence-rate on the corresponding single-photon detector at Bob (+45°) using the bat-ears of the P/M-base. This will align the P/M base.

Instead of minimizing the corresponding detector, the target-state would also allow to maximize the opposite detector (e.g maximize the H-detector when Alice triggers only V photons). As mentioned, the minimum is detector dependent whereas the maximum depends on the attenuation of the quantum channel. Using the minimum has the advantage that it allows to evaluate the alignment process independent of the fibre losses, i.e. for different fibres.

6.2.2. Preparations for the automatic alignment

For a hands-off QKD system, it is necessary to automatise the whole alignment process. For this purpose, the manual polarisation controllers were replaced by electronic polarisation controllers (General Photonics PolaRite II [36], see fig. 6.4). The controllers consist of four piezo-based squeezers orientated 45° with respect to each other. It also includes a DC/DC converter and high-voltage amplifier accepting analogue inputs from 0 to 5V.

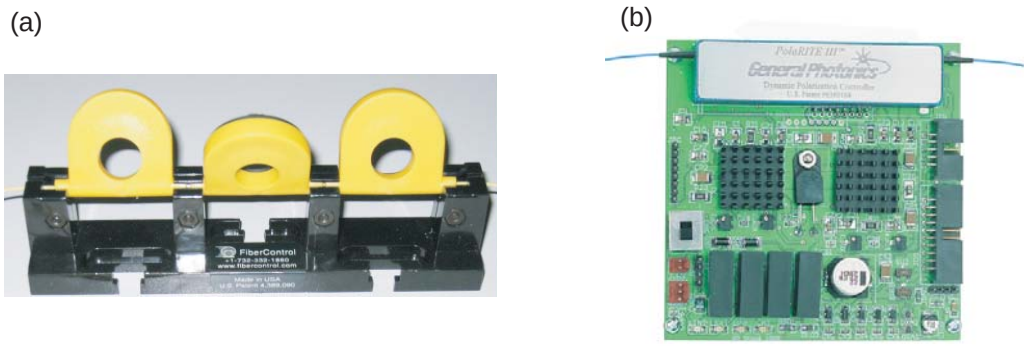

Figure 6.4.: (a) Manual "bat-ears" polarisation controller. Three fibre loops are turned with respect to each other to rotate the polarisation.
(b) PolaRite II polarisation controller module (picture taken from [36]). Four piezo motors squeeze the fibre and hence induce birefringence rotating the polarisation. The module also includes a DC/DC converter and high-voltage amplifier accepting analogue inputs.

[5] note that all other photons are still detected but will not contribute to trigger pulses and hence no coincidences on Bob's detectors

As shown in figure 5.1, the first polarisation controller (PC1) is located before Bob's fibre-based BB84 module and is shared with the polarisation control module (PolCtrl) described in the next chapter. PC1 is used to align the P/M basis. The second polarisation controller PC2 is used to align the H/V basis i.e. to rotate the measurement axis by 45°with respect to the P/M basis. PolBob includes a 12-bit DAC with 8 channels to access all analogue inputs of both polarisation controllers.

6.2.3. Preliminary tests

Before implementing the automatic alignment procedure on PolBob we made some preliminary tests with the polarisation controllers to determine suitable step sizes, averaging times etc. Unfortunately, we discovered significant hytereses effects on all channels of the polarisation controllers as shown in figure 6.5.

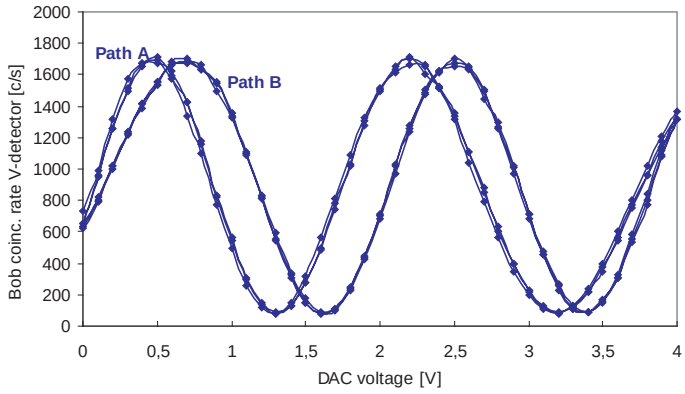

Figure 6.5.: Coincidence rate on the V-detector when the voltage is changed on one channel of the polarisation controller. Alice here triggers only on vertical photons. In this scheme, the H/V basis in the BB84 module acts as a polarisation analyser. One can see that there is a large difference in the change of polarisation caused by the polarisation controller for different paths (path A: 0V→4V, path B: 4V→0V) caused by hystersis effects in the PolaRite controller.

Further tests showed that it is not possible to avoid the hysteresis effect since all channels of the PolaRite module are affected. However, it is possible to reduce the effect by restricting the voltage range and step sizes. Furthermore it is important to avoid large voltage jumps. We also noticed that the difference in the transformation due to the hysteresis is not equal for every channel.

This is not a particular problem for the state alignment module because the procedure itself uses an algorithm (once again the Hill Climber) that tries to keep the voltage-steps as small as possible and avoids bidirectional jumps on the DAC channel. But it is indeed a problem for the polarisation control module (PolCtrl) described in the next section.

6.2.4. Automatic alignment procedure

At the beginning, all eight DAC channels are set to the middle of the range (2V). The procedure of the automatic version of the alignment process (StateAlign) is in principle very similar to the manual process:

1. Tell Alice to send trigger pulses only when the detection event comes from the +45°detector. For this purpose, electronic switches have been installed on Alice to enable each channel separately. These switches are accessible using certain QSH commands[6].
2. To align the P/M basis, PolBob tries to minimise the count rate of Bob's +45°(P) detector by the using the first polarisation controller. Note that every change on PC1 also effects the H/V basis.
3. Tell Alice to trigger only on vertically measured photons
4. PolBob uses the second polarisation controller to minimise the count rate on the V detector. This will align the H/V basis.

Note that the order of aligning the bases (P/M, then H/V) is given by the arrangement of the polarisation controllers (see fig. 5.1).

To find the minimum count rate on one detector, the same Hill-Climber algorithm (6.1.1) as used for SourceStab has been implemented on PolBob. Instead of moving the piezo-channels, here the voltage on the DAC-channels is changed. Another difference is that PolBob searches for a minimum instead of a maximum. The principal scheme stays the same.

PolBob receives the single photon count rate every second from Bob via UDP. If the count rate is above a certain threshold (150 c/s), larger voltage steps (150mV) and shorter averaging times (3 seconds) are used. Otherwise PolBob applies small voltage steps (40mV) and uses a longer averaging time (10 seconds). Initial tests showed that smaller voltage steps or shorter averaging time can cause wrong behaviour because of the unavoidable fluctuation (noise) of the count rate. Similar to SourceStab, PolBob will use all four channels of the polarisation controller consecutively to reach the minimum. An example of an alignment process is shown in figure 6.6.

The whole alignment process takes about 3 - 5 minutes for one basis. It can happen that the previously aligned P/M base will drift away during the alignment process of the H/V base. For example because of mechanical fluctuations in the fibre or temperature changes. Therefore, the alignment will be repeated for both bases. During the second run, detector specific thresholds are introduced. If the count rate on the monitored detector falls below this value, the alignment process for this basis is considered successful and the remaining DAC channels are skipped. This will usually reduce the necessary time for aligning the basis to below one minute.

Compared to the manual alignment, the automatic version (StateAlign) takes longer, but it has several advantages. First of all, it achieves significantly more reliable results because of the

[6]The QSH (Quantum Shell) is an interface to the FPGA registers, a list of commands for the alignment process is given in [38].

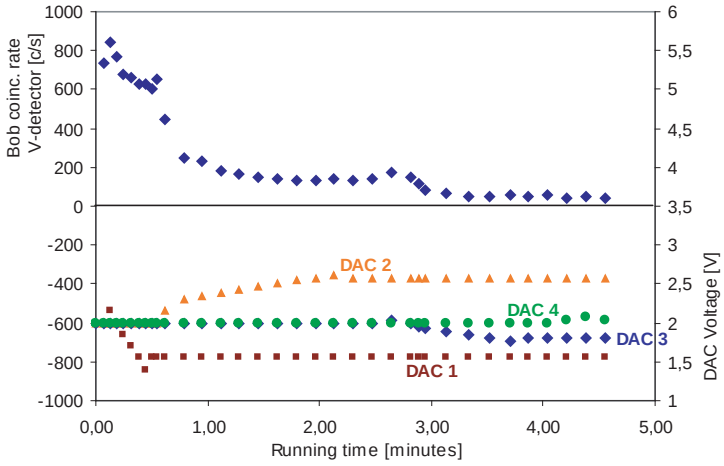

Figure 6.6.: The implementation of the Hill Climber algorithm allows to minimise the coincidence rate on the target detector (here: V) using all four channels (DAC 1-4) of the polarisation controller when Alice triggers only vertically measured photons. This will align the target state $|\psi^-\rangle$ in the H/V basis.

long averaging time (microprocessors are more patient than humans). Furthermore, the electronic polarisation controller allows making more accurate changes than the manual controllers because even slightly touching the polarisation controller applies some pressure on the fibre and will hence change the polarisation. Another advantage is that this procedure allows to easily align the target state independent of the relative phase in the entangled state since we use two independent polarisation controllers for the two bases. The phase does not change the behaviour when both photons are measured in the H/V basis but changes the correlations of the state in a different basis (e.g. P/M).

6.2.5. Automatic polarisation re-alignment

The PolCtrl module described in the next chapter is used to keep the polarisation stable once the entangled state is aligned. PolCtrl can compensate polarisation drifts inside the fibre but not drifts in several other parts in the system. The fibre that connects the 810nm output of the entanglement source with the free space BB84 module and Bob's completely fibre based BB84 module are completely uncompensated and therefore prone to temperature changes. As a consequence, the polarisation alignment will be lost and the QBER will start to rise. As pointed out in chapter 8.4, this has been a large problem during the SECOQC demonstration because the room temperatures changed up to 10°C within a 24h cycle. The laid-out fibre itself is rather stable[7]. Using the automated state alignment, even these drifts can be corrected! For this purpose, the management module (see section 6.5) monitors the QBER and starts the re-alignment of the state if the QBER rises above a certain threshold (e.g. 1% above the initial value after the first polarisation alignment). The only difference to the normal alignment process is that the DAC-channels are not initialised to 2V but start with the previous voltages. Note

that it is very important that the QKD must not run during the (re-)alignment process! Because Alice triggers only one detector (V or P) the acquired raw key string would be a sequence of the same bit (e.g. 1111 ...) which is definitely not secure.

6.3. Polarisation Control (PolCtrl)

The module in the previous chapter (StateAlign) described how the desired entangled state is aligned automatically. In a real world scenario, the laid-out fibre is exposed to several temporal fluctuations. The birefringence of the fibre causes arbitrary polarisation transformation depending on environmental factors like temperature and/or mechanical stress. The transformation in the quantum channel is unitary and hence can be compensated using a singe polarisation controller at the end of the quantum channel.

Therefore, another stabilisation module is required to compensate the temporal polarisation drifts of the fibre and keep the quantum channel stable. This requirement has been recognised already several years ago. Bernhard Schenk developed the first prototype of a polarisation control (PolCtrl) using strong reference pulses within his diploma thesis[6]. This approach has been further developed by Thorben Kelling[7] and Daniele Ferrini[8].

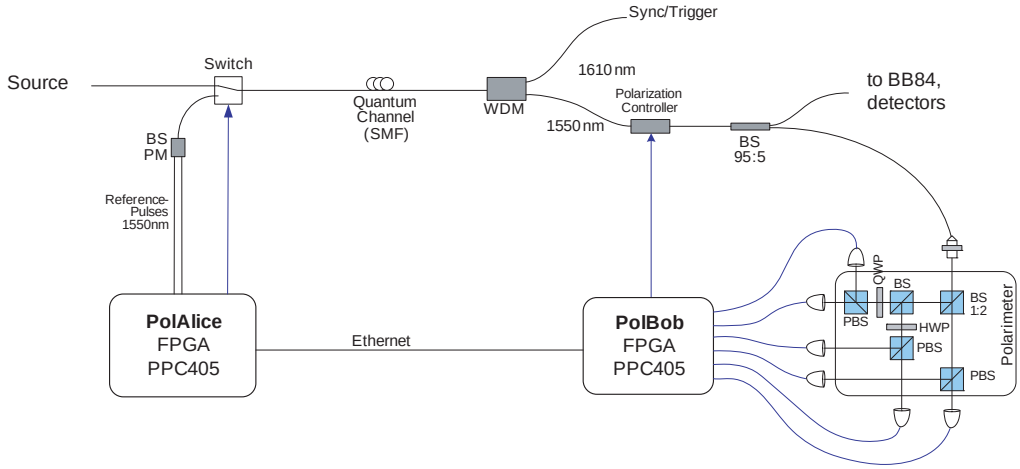

Figure 6.7.: Details of the components used for the PolCtrl module

PolAlice includes two reference diodes at 1550nm (the same wavelength as the single photons) with fixed polarisations (H and P) that are connected to polarisation maintaining fibres, coupled together using a beam splitter and connected to a fibre switch that is controlled by PolAlice. On Bob's side, a 95/5 fibre beam splitter is used to direct a fraction of the light from the quantum channel to a six-channel polarimeter. The incoming light is devided into three equal parts. Each part is analysed in the two linear (H/V and P/M) and the circular (R/L) basis. PolBob uses six photo diodes to measure the power of the components at the outputs and calculates the Stokes parameters[7]. The four-channel polarisation controller PC1 is used to keep the polarisation stable.

[7] a short overview on the description of classical polarisation using the Stokes parameters is given in appendix B

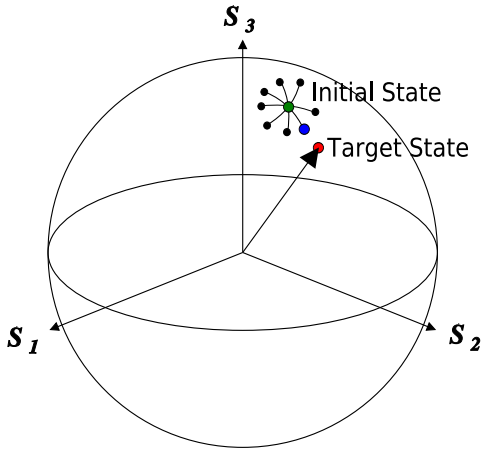

Figure 6.8.: Principle scheme of PolCtrl on the Poincaré sphere. PolBob applies eight deviations on the four inputs of the polarisation controller in the quantum channel. At the end of the cycle, the state that is closest to the target state is chosen.

6.3.1. Polarisation stabilisation procedure

Details of the polarisation control (PolCtrl) procedure can be found in the diploma thesis mentioned above [6, 7, 8]. Here, only the basic procedure of the PolCtrl cycle is sketched:

1. PolBob asks PolAlice to send a pair of reference pulses: horizontal(H) and +45°(P)
2. PolAlice tells Alice to stop sending trigger pulses and stop QKD using a TTL signal
3. PolAlice switches the quantum channel to the reference diodes
4. PolAlice sends a short horizontal (H) pulse (30ms)
5. PolBob waits for the H-pulse
6. PolBob applies a series of voltages (8 deviations) on the 4 DAC channels of the first polarisation controller during the H-pulse (black lines in figure 6.8). The voltage is increased by one step-size (5mV) and decreased by one step-size for each channel consecutively.
7. PolBob measures the polarisation of the initial state (green point in figure 6.8) and after each deviation. He calculates a set of Stokes parameters for all nine states.
8. PolAlice sends a short +45°(P) pulse (30ms)
9. PolBob applies the same series of voltages during the P-pulse and obtains another set of Stokes parameters.
10. PolBob calculates the deviation angles to the target state for all nine voltage settings for each pulse separately
11. PolBob applies the voltage that corresponds to the smallest angular distance to the target state (blue point in fig. 6.8). Note that the distance for both consecutive reference pulses (H and P) to the target state must be minimised. For each pulse, a separate target state is

defined. Therefore, the common deviation is calculated for all nine points: $\theta_i = \sqrt{\theta_{H,i}^2 + \theta_{P,i}^2}$ where $\theta_{H,i}^2$ is the angular distance between the H-pulse and H-target for deviation number i. The voltage at the end of the PolCtrl cycle is set to the smallest common deviation.

12. PolBob requests more reference pulses dependent on the deviation angle to the target state and repeats the steps 1-11

13. PolAlice waits some time, switches the quantum channel back to the entanglement source and tells Alice to continue QKD

The whole cycle takes about 250ms. To stabilise the channel, the complete cycle needs to be repeated periodically. Too fast repetition rates will decrease the final key rate because the QKD needs to be stopped during the cycle. Short-term fluctuations (e.g. when somebody touches the fibre) can be covered when the QBER is monitored by the management module (see section 6.5).

6.3.2. Measuring the target state

The previous version of PolCtrl was based on keeping a predefined target state. The polarisation state of the reference diodes should be mapped to the same state after transmission.

$$H \longrightarrow H = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad P \longrightarrow P = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{6.2}$$

After the first PolCtrl cycle, the entangled state was aligned manually as described in the last chapter. This is not applicable any more since the first polarisation controller is shared by the state alignment module StateAlign and PolCtrl. Hence, the target state on the polarimeter will be an arbitrary state after the polarisation entangled state is aligned.

A procedure to measure the target states immediately after the state alignment is therefore necessary:

1. Renormalisation (see next paragraph)

2. Request a long pair of reference pulses (each one second) from PolAlice

3. Measure the polarisation of both pulses at the fibre output by averaging over the whole duration of the reference pulse.

4. Set the measured states as the new target states

In the normal start-up sequence of the QKD system, the actual QKD is started immediately after the target state is measured to avoid further polarisation drifts.

6.3.3. New renormalisation procedure

Before calculating the stokes parameters from the diode voltages, one needs to normalise the receiver diodes (see [7] for details). This is done by requesting a pair of reference pulses (each 3.5s) and searching for a minimum on each photo diode (having a minimum on one diode, e.g. V, corresponds to a maximum on the opposite diode in this basis, e.g. H). The minimum and maximum voltages are stored and later used to calculate the normalised stokes parameters (see appendix B, eqn. B.7).

At the end of the procedure, the DAC voltages are restored to the original values to obtain the same polarisation transformation as before the normalisation. Unfortunately, this is not possible in practice because of the hysteresis in the PolaRite polarisation controller. The last step will always lead to a different transformation away from the target state.

It is evident, that the normalisation should be carried out before the target state is measured. If not even the target state is correctly measured, the polarisation control is doomed to failure. Unfortunately, we noticed that the normalisation procedure destroys the previously aligned state because of the problem mentioned in the previous paragraph. Since temperature fluctuation change the bias voltage of PolBob's receiver diodes, a periodic re-normalisation is however necessary. This brings us in a dilemma: we cannot use the normalisation procedure because of the problem with the hysteresis which leads to unwanted changes in the polarisation and hence higher QBER. On the other hand, we need to execute normalisations periodically and always before measuring the target state.

Therefore, a new approach for the periodic re-normalisation is implemented in this thesis: Since minimum and maximum are related to the bias voltage of the amplifier, the idea is to use the bias voltage itself to handle temperature fluctuations. Only the initial normalisation values obtained at the system start-up are kept.

The new renormalisation procedure measures the bias voltage when the fibre is dark (i.e. no classical light pulses). The minimum and maximum voltages acquired during start-up-normalisation are subsequently adjusted parallel to changes of the bias voltage. E.g. when the bias voltage of a certain detector changes by 50mV, we assume that minimum and maximum voltages also change by 50mV in the same direction.

A test measurement over 60 hours supports this approach. During the measurement, minima and maxima determined by the normalisation routine drifted parallel to the bias voltage as shown in fig. 6.9. The maximum changes slightly more then the bias voltage since the amplification factor is also temperature dependent. This can be considered by using a constant factor when the maxima are changed.

This way of renormalisation allows to avoid the large jump on the DAC channels that occurs after the normalisation procedure. Furthermore, the bias voltages can be measured during normal QKD operation, single photons will not influence the receiver diodes of the polarimeter.

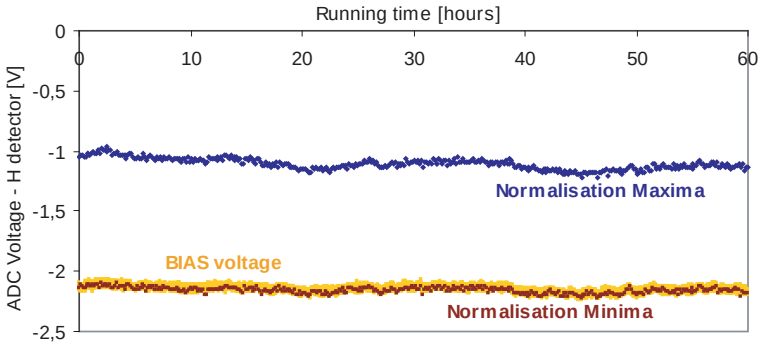

Figure 6.9.: Detector bias voltage compared to minimum and maximum voltage acquired by the normalisation procedure during a 60h test run

6.3.4. Laboratory tests

We tested the polarisation stabilisation module by putting the fibre spool outside a window to simulate the real-world temperature influence on the fibre. Alice and Bob were placed in a room with stable temperature to rule out the temperature influence on the synchronisation circuits.

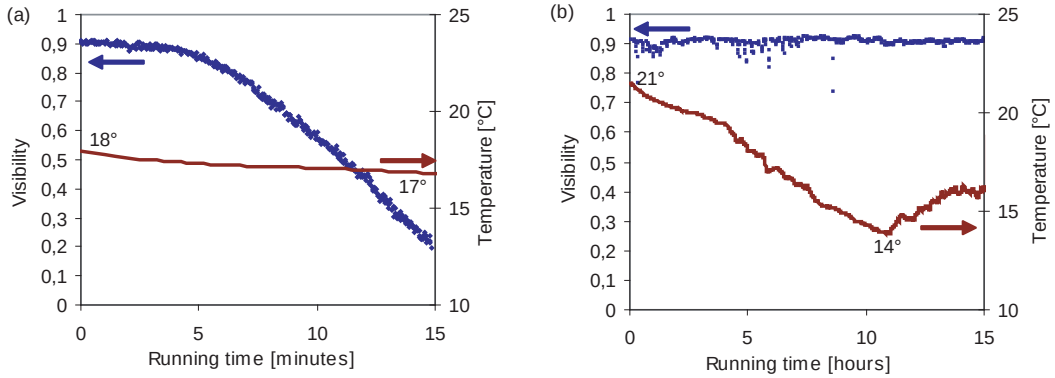

Figure 6.10.: Visibility and temperature during a test with a 25km fibre spool placed outside a window.
(a) Visibility and temperature for test run without PolCtrl.
(b) repeated measurement with PolCtrl turned on.

The visibility is defined as $V = \frac{max-min}{max+min}$ where max is the maximal coincidence rate for orthogonal polariser settings[8] at Alice and Bob and min the minimal coincidence rate for parallel polariser settings.

First, we made a (short) run without PolCtrl. One can see the large influence of the temperature on the visibility. Even a small change in temperature ($\sim$1.5°C) completely destroys the entangled state within 15 minutes.

[8]The state-align module aligns the state to $|\psi^-\rangle$. Hence the maximal coincidence rate is obtained for orthogonal polariser settings.

We repeated the measurement with PolCtrl turned on. The visibility stayed stable around 90% although the temperature changed more than during the first run (∼7°C). The remaining spikes are believed to result from the hysteresis effects in the polarisation controller.

6.3.5. Open problems

One disadvantage (among others) in the current approach for polarisation stabilisation is that PolCtrl relies on applying the same voltage series on two consecutive reference pulses. In the current scheme, eight voltage steps are applied on the controller channels. After each deviation, the voltage is put back the initial value before the cycle. For example, the pattern which is applied to every channel looks like 2V → 2.05V → 2V → 1.95V → 2V.

The authors of the original scheme [6, 7, 8] assumed, that the polarisation controller applies the same transformation when the same voltage is applied, i.e. applies the same transformation before and after the voltage step. Due to the hysteresis of the PolaRite controller this is not possible for even one step, not to mention sixteen consecutive steps.

On the other hand it not possible to use only one reference pulse. If one point on the Poincar sphere is fixed it is still possible to rotate the whole sphere around the axis defined by the origin and the fixed point itself. Due to the two-basis concept of QKD, the whole sphere needs to be stabilised. Therefore, it is inevitable to fix two points on the sphere, i.e. use two non-orthogonal reference pulses.

The previous version of PolCtrl used a distance dependent step multiplier to increase the voltage steps if the state is far away from the target. Certainly this is rather counterproductive because larger voltage steps will also expose the hystersis effects more. Instead of using a variable step size, we now use more pulses to get closer to the target state. This approach takes a bit longer but leads to significantly better results.

Figure 6.11 shows the behaviour of PolCtrl during the two-weeks demonstration of the SECOQC network. One can identify three problems:

- The normalisation procedure does not work always correctly (normalised stokes parameters should be smaller than 1)
- From hour 171 to 173.5, the polarisation measured at the polarimeter was very stable. Nevertheless, the management module initialised a realignment of the entangled state because the QBER reached the threshold (see sec. 6.5.3). This behaviour has been expected because the large temperature deviations in Bob's room leads to polarisation drifts in parts of the system that cannot be stabilised.
- PolCtrl fails to keep the target state during the hours 174.5 and 177. One can see that the distance to the target state steadily increases. At the moment, we believe that this is due to the inherent problem with the hysteresis that leads to the misbehaviour. Again, it is the management module that recognises the increased QBER and starts a re-alignment of the entangled state.

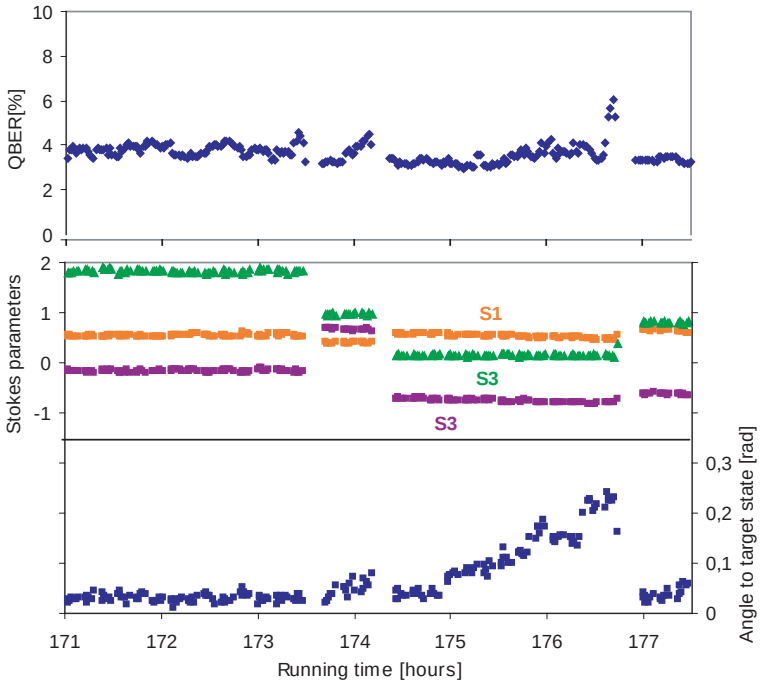

Figure 6.11.: Stokes parameters and the distance to the target state during the SECOQC test phase. The zero-point on the x-axis is referred to October 8th 2008, the date of the SECOQC conference.

Tests with rather large external influences on the fibre, e.g. mechanically moving the fibre or putting the fibre under strong temperature changes showed that PolCtrl works fine in principle. However, the problem seems to be at smaller changes around a stable polarisation as it is in the laid-out fibre. In this case, the hysteresis becomes the dominant effect and leads to an unwanted drift in the polarisation.

At the moment, the second largest problem of the current approach (beside the hysteresis) is that drifts in several optical components cannot be compensated (see section 6.2.5). This especially is a problem in an environment without temperature stabilisation. From fig. 6.11, one can see that the target state after the re-alignment of the entangled state changes a lot during a period of six hours. The polarisation drifts in the laid-out fibre we used for the SECOQC network demonstration were however significantly lower on a 24h period[9]. We believe that this is because of the temperature influences on the fibre-based BB84 module which cannot be compensated by PolCtrl.

We furthermore recognised a high QBER peak immediately after the PolCtrl cycle. This comes along with a peak on the detection rate on Bob's side. We believe that the strong reference pulse (95% of the reference pulse enter the BB84 module, only a fraction of 5% enters the polarimeter) heat up the InGaAs diodes (which are not triggered but stay in linear mode) leading to higher dark count rates for a short time. The only way to prevent this QBER peak is to set the delay

[9]See for example [7] where several polarisation measurements of the fibre links are shown.

time sufficiently long (∼150ms) before PolAlice switches the quantum channel back to the source. This blocks the quantum channel and hence the QKD process for a longer time than the actual reference pulses (150ms vs. 60ms).

Presently, the possibility of automatically re-aligning the entangled state allow to compensate the problems described above when the QBER starts to rise. However, there are some alternative approaches that should be tested:

- General Photonics suggests [39] to drive the controller with direction dependent different voltage steps to overcome the hysteresis problem.
- Drive every voltage needed for the polarisation control over the same path. This would take significantly longer and therefore also block the quantum channel for a longer time.
- A completely different approach on the polarisation control issue like a QBER based algorithm described in sec. 9.3.

6.4. Detector Synchronisation (FindDelay/FindWindow)

The gate width of Bob's InGaAs detectors should be as short as possible (∼1ns) to reduce unwanted detection events (dark counts and accidental coincidences). This requires absolute precise timing to synchronise the gate with the arrival of the photon. On a long-term scale, temperature fluctuations have an effect on the runtime of the electronic trigger pulses in Alice and Bob[10] leading to a loss of count rates. Therefore, periodic resynchronisation is necessary.

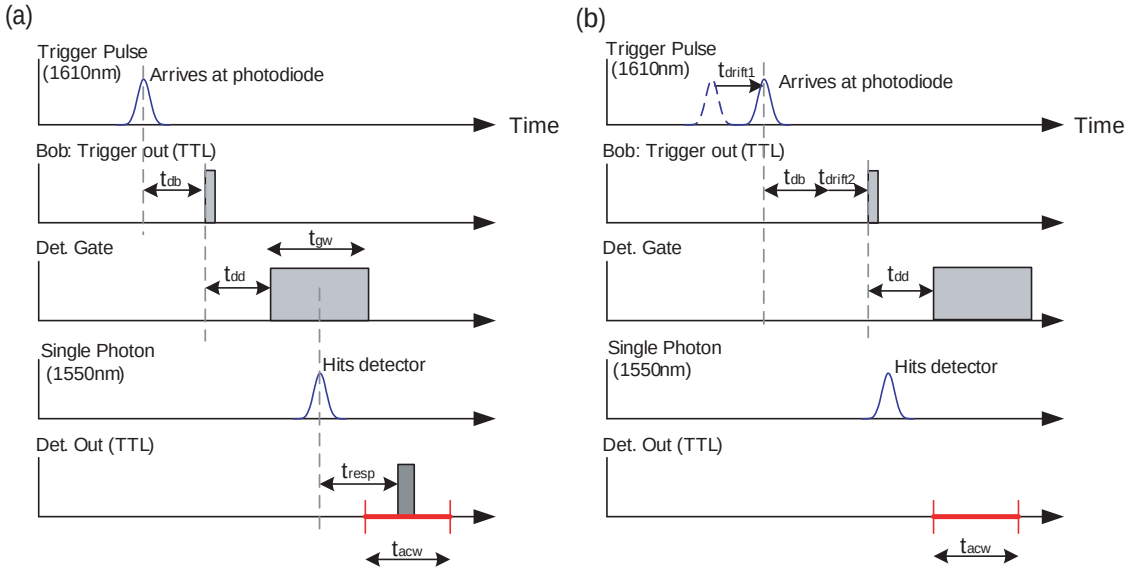

Figure 6.12.: Timing sequence for detector synchronisation on Bob's side
(a) In the fibre, the optical trigger pulse follows the single photon. After the arrival of the optical trigger pulse, the TTL output (from Bob to detector) is delayed individually for every detector (t_{db}). The gate on the APD is applied after some internal delay (t_{dd}). The gate width t_{gw} is about 1.5ns. If the detector is synchronised perfectly, the photon arrives in the centre of the detector gate. t_{resp} is the response time of the detector (∼20ns), t_{acw} is the auxiliary coincidence window which is explained later.
(b) A drift in the trigger-circuits in Alice t_{drift1} and/or Bob t_{drift2} delays the trigger pulse and cause the photon to fall out of the gate. The photon will not be detected. Hence, a re-sychronisation is necessary. In this example, the internal delay and the positions for the auxiliary coincidence window need to be adapted.

To accomplish the required precision for detector synchronisation, Alice and Bob include individual delay lines with a resolution of 10ps and a range of 10ns for each detector channel.

- On Alice, the optical trigger pulse is delayed after a detector event arrived from the Si-APD modules (TTL). For each detector channel an individual delay line is available.
- On Bob, the arriving trigger pulse is delayed individually before it is passed to the detector's gate input (TTL).

[10] During the SECOQC demonstration, we experienced a fluctuation of about 120 ps/degree and a total fluctuation of about 1.2ns on a 24h scale, see fig. 6.14

6.4.1. Delay adjustment

The chromatic dispersion of the fibre will cause the trigger pulse (1610nm) to lag behind the single photon (1550nm). Table 6.2 gives an overview of the time-difference between trigger pulse and photon caused by dispersion in different fibres.

For example, when the 25km fibre spool (NZDS, non-zero dispersion shifted fibre) used for laboratory tests is replaced by the 16km fibre between Siemensstrasse (SIE) and Erdberg (ERD)[11], one needs to compensate an additional 11.7ns. This is more then the range of the electronic delay lines (10ns). Therefore, we use a delay fibre in Alice for a coarse delay adjustment. In the example above, a 2m (10ns) piece of fibre is suitable. Note that the delay fibre is the only (!) element in the complete QKD system that needs to be adapted when the length of the quantum channel is changed. Unfortunately it is not yet possible to replace the delay fibre with a different delay chip with a longer range or a concatenation of the already used type due to the increase of timing jitter.

Fibre	Dispersion Coeff. [ps/nm/km]	Total Dispersion [ns]
25km NZDS	5	7,5
50km NZDS	5	15,0
75km NZDS	5	22,5
16km Standard	20	19,2
32km Standard	20	38,4

Table 6.2.: Time difference caused by dispersion between single photon (1550nm) and trigger pulse (1610nm) for some fibre links. The 16km link is the one we have used during the SECOQC conference.

The delay lines on Alice and Bob are accessible over the QSH (Quantum Shell), an interface to the FPGA registers. At the beginning of 2008, the QSH commands had to be entered manually to a certain QSH-File. This is very impracticable even for a laboratory environment. Every time a delay line needs to be adjusted (e.g. due to temperature changes), the QSH files had to be changed and the QKD restarted consecutively. To find the best delay value (highest count rates) several restarts lasting for several minutes were necessary.

We therefore developed the QKD Control Client. A program written in Java that allows to adjust several parameters like the delay-lines, the position of the time-window (see next section), size of the sifted key etc. in a very convenient way. In combination with the QKD Monitor (see sec. A.2), the QKD Control Client furthermore allows to automatically find the correct delay to achieve maximum count rates.

Although very convenient, this way of detector synchronisation has some disadvantages:

- The QKD Control Client uses the count rates that the QKD Monitor receives from Bob

[11] This is the fibre link we have used during the SECOQC network demonstration

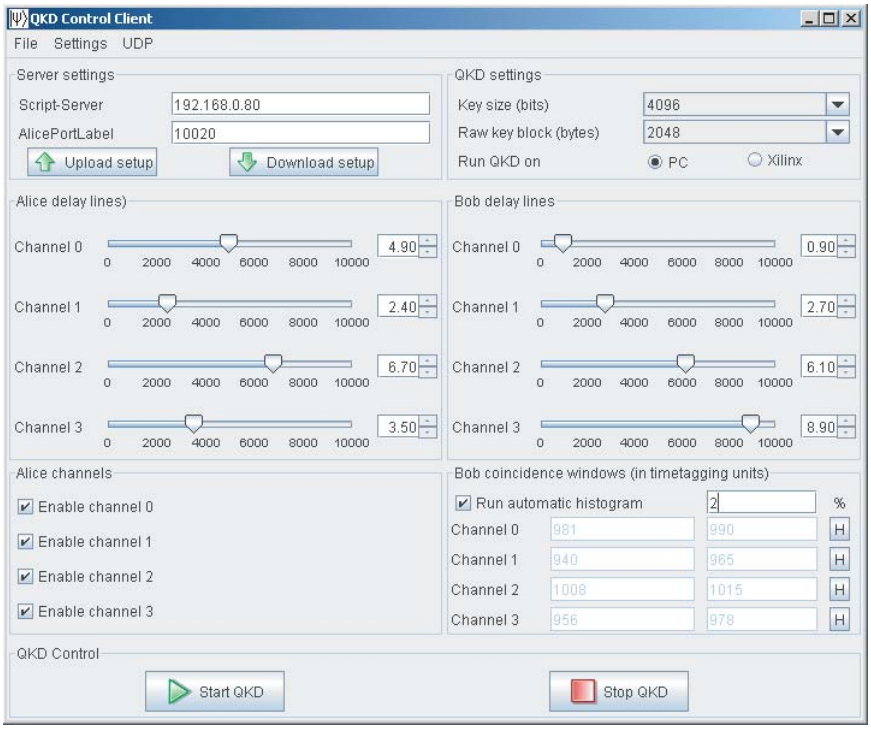

Figure 6.13.: The QKD Control Client, a program written in Java allows to set the delay lines on Alice and Bob, to enable detector channels on Alice and to set the auxiliary coincidence windows on Bob

and tries to maximise the count rates sending commands to Bob. It is obvious that the whole procedure could run directly on Bob without further communication[12].

- The QKD Monitor is - as the name suggests - a monitoring program and should not be used as a part of the automation/stabilisation procedures.
- It is not possible to integrate the QKD Control Client in the overall system architecture of the QKD system where every module is coordinated by the mangement module (see section 6.5).

In collaboration with the Austrian Research Centers a program called FindDelay has been developed. It is running directly on Bob and scans the whole delay-range and searches for a maximal count rate. In a second run, a smaller range (1ns) around the maxima and longer averaging times are used to precisely locate the maximum. FindDelay is able to scan all four detectors parallel and takes about 90 seconds. Figure 6.14 shows the coincidence rates on Bob's detectors during the FindDelay search.

To achieve a precise synchronisation between photon and detector gate, the delay lines on Bob are used. Each detector needs to be adjusted individually because of slightly different runtimes inside the detector. This is a very important step, not just to achieve a high count rate but also

[12]The QKD system already requires a lot of communication between the components (Alice, Bob, PolAlice, PolBob), we therefore tried to avoid unnecessary communication

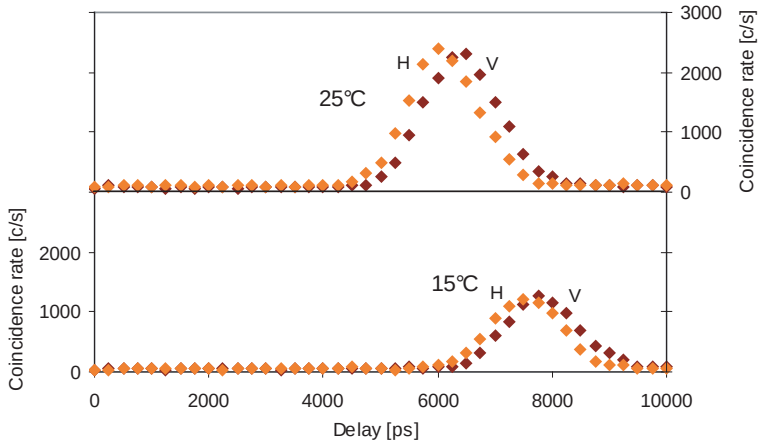

Figure 6.14.: Top: Coincidence rates (H and V) during the FindDelay run at 25°C. One can see that the detectors have a timing-mismatch of about 500ps caused by differences in the internal delay. Without precise timing, the difference would make the QKD system prone to the time-shift attack (see section 9.4.3).
Bottom: FindDelay-run at 15°C. The temperature difference causes a drift in the runtime of the trigger-circuits of 1.2ns. The decrease of the peak coincidence rate results from a temperature dependence of the idQuantique detectors (see sec. 8.4.1)

to counter several side channel attacks. The first technically feasible side channel attacks expose unequal timing adjustment to make the detectors distinguishable[13].

6.4.2. Auxiliary coincidence window (FindWindow)

The primary coincidence window is of course the gate of the InGaAs detector. During the tests in the laboratory, we used a detector build by the KTH Stockholm that has a rather broad and fixed gate width of about 5ns. Therefore, this detector is more prone to dark counts and accidental coincidences than the id200 detectors (with a gate of ∼1.5ns). We can however use an auxiliary coincidence window to filter out a fraction of the unwanted coincidence events. The incoming trigger pulse starts a time-tagging unit (TTU) with a resolution of 82ps built by the Austrian Research Centers (ARC). Only the coincidence events from the detector that arrive within a certain time-window will be considered. All other events will be ignored.

To set the time window correctly, the time-distribution of the detector output has to be measured first. Thus, Bob measures the time between the arrival of the trigger pulse and the detection event in time-tagging units (82ps). In a special histogram-mode, Bob will create a histogram containing the number of coincidences arrived per time-tagging unit (TTU). The histogram can be analysed to find the centre of the auxiliary coincidence window. To avoid side channel attacks, the coincidence window must have the same width for every detector channel.

Similar to the situation for the delay-lines, the coincidence windows have to be set using certain

[13]This attack and it's implications on our system will be discussed in a later section 9.4

QSH-commands. For the laboratory prototype, the QKD Control Client allowed to analyse the coincidence histogram created by Bob and subsequently sets the coincidence window automatically. Alternatively, the coincidence window can be set manually for each detector. In collaboration with the Austrian Research Centers, the FindWindow program has been developed. It automatically generates the coincidence histogram for every channel, analyses the histogram and sets the coincidence window with a given width around the maximum.

Since FindDelay and FindWindow run directly on Bob, both procedures can be integrated into the management module architecture (see section 6.5). The management module coordinates the complete QKD system and will be described in the next chapter.

6.4.3. Periodic delay re-synchronisation

As mentioned above, the runtime of the trigger circuits is temperature dependent. Therefore a periodic re-synchronisation is necessary to compensate drifts (see fig. 6.12). In this mode, FindDelay searches locally for higher count rates. The position of the auxiliary coincidence window are moved parallel to the delay-drift. To compensate the temperature fluctuations, it is sufficient to run the FindDelay re-synchronisation every 10 minutes.

6.5. Management Module

With the modules described in the last sections, we are able to:

- Automatically adjust and stabilise the entanglement source to maximal count rates (SourceStab)
- Automatically align the desired entangled state (StateAlign)
- Automatically synchronise the InGaAs detector gates with the arriving photons (FindDelay/FindWindow)
- Keep the polarisation stable at the fibre output (PolCtrl)

To achieve a hands-off start-up, stable and automatic operation of the QKD system, a precise and reliable coordination of the modules is required. For these purposes we have conceived the so-called management module (MM) in collaboration with the Austrian Research Centers. Technical details can be found in the specification document [38]. It is a master-slave state machine (Alice is master), that runs on the node computers. An overview of the management module's tasks is given here.

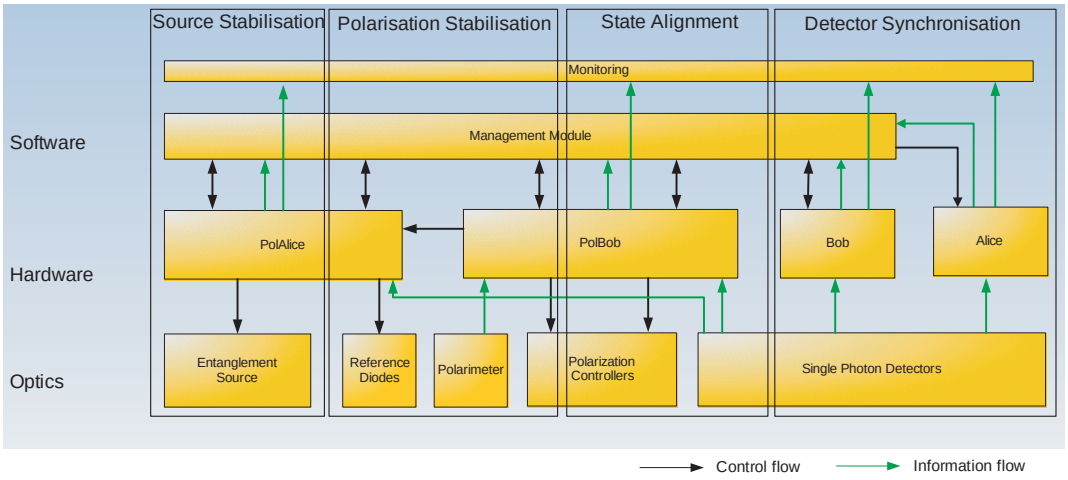

Figure 6.15.: Overview of the architecture of the management module (MM). The MM will coordinate and control all other components in the QKD system.

The MM has to take care that only one module is running at a time. The correct operation of the modules is not possible when two modules work in parallel. For example: a PolCtrl cycle stops Alice for a fraction of a second because the quantum channel is switched to the reference diodes. This leads to a lower count rate for a short time and hence could cause a wrong behaviour of SourceStab, FindDelay, FindWindow and StateAlign. In some cases, the situation gets even more complicated because several components are involved and the control structures between them have to be considered. For example, figure 6.16 shows the sequence diagram for a complete state alignment procedure. Again, it is the MM that takes care of the correct order. Similar sequence diagrams for the other modules can be found in MM specification [38].

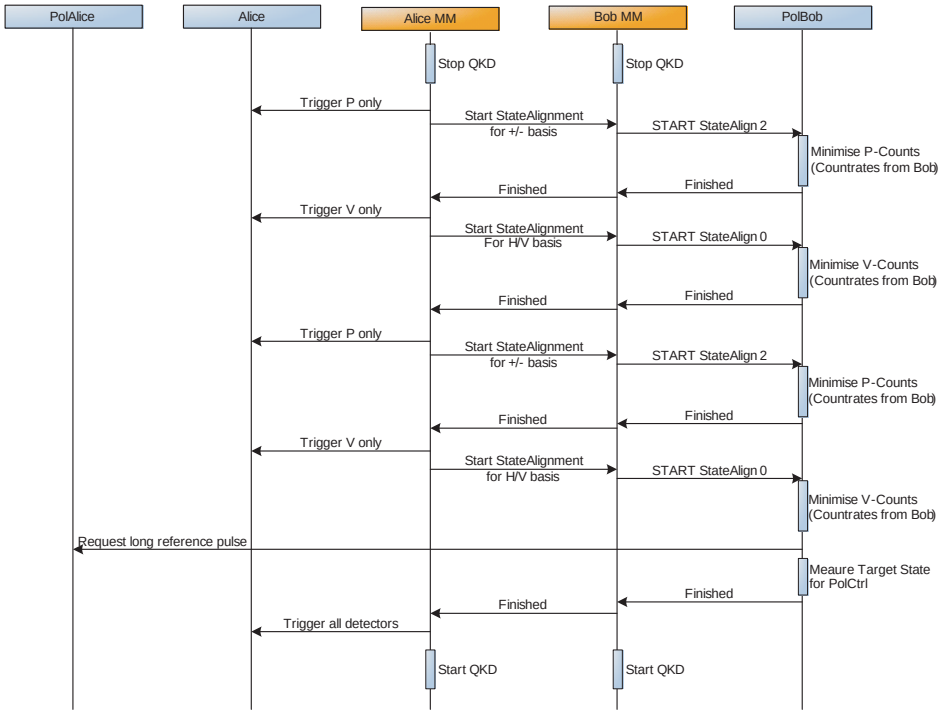

Figure 6.16.: Sequence diagram for the state alignment module (see section 6.2). During the whole process, Bob sends his coincidence rates every second to PolBob.

6.5.1. Start-up process

The management module coordinates all components that are necessary for a hands-off start-up of the QKD system. For the start-up process, the correct sequence is very important. As an example, SourceStab will not work correctly if the detector synchronisation (FindDelay, FindWindow) is not completed. The sequence looks as follows:

1. Start Alice and Bob (without QKD)
2. Is-alive check for PolAlice and PolBob
3. FindDelay (global version for full delay-scan)
4. FindWindow
5. SourceStab (quick mode with larger steps)
6. PolCtrl normalisation
7. StateAlign (includes measuring the target state)
8. Start QKD

A typical start-up takes about 15-20 minutes. Even after transporting the complete system, the start-up takes not more than 25 minutes (see fig. 6.17). Because of the frequent restarts of the

nodes during the SECOQC demonstration, we usually skip SourceStab (in quick start mode) when the system is restarted. This reduces the time for a restart of the system to about 10 min.

6.5.2. Normal QKD operation

As pointed out in the previous chapters, some of the modules need to run periodically to guarantee a stable key generation. Therefore, the management module will call the modules in a certain sequence:

1. FindDelay (resynchronisation)
2. SourceStab (small step size)
3. PolCtrl renormalisation
4. Ten PolCtrl cycles with an interval of 10 seconds
5. Ten PolCtrl cycles with an interval of 30 seconds

This basic cycle takes about 10 minutes will be repeated in an infinite loop, until an error occurs.

6.5.3. Error handling

The stabilisation modules are conceived to compensate most of the real-life fluctuations. However, some effects cannot be compensated within the normal cycle. In some cases, the MM can detect the problem and try to handle it. In some cases, the key generation needs to be stopped because the security of the key cannot be guaranteed any more (e.g. when one of the detectors fails). The link operator will be informed via e-mail if it is not possible to solve the problem automatically. Here is a list of error scenarios that are currently covered by the management module:

- When somebody incidentally touches the fibre, the QBER will suddenly increase. In this case, the MM stops the normal operation cycle and immediately starts several PolCtrl cycles to compensate the change as fast as possible. If this does not help, the MM initiates a re-alignment of the entangled state.
- As mentioned in the previous chapters, temperature fluctuations in Bob will lead to polarisation drifts that cannot be compensated by PolCtrl. In addition, PolCtrl is not able to compensate all drifts in the fibre because of the hystersis in the polarisation controller. Both effects will lead to a slow rise of the QBER. Therefore, the management module measures the QBER immediately after the start-up. If the QBER exceeds a certain threshold (start-value + 1%), a re-alignment of the entangled state is started which brings the QBER back again to a low value [14].

[14] During the SECOQC demonstration, where no air-conditioning has been available and the temperature fluctuated heavily, a re-aligned was necessary on average every 2.5 hours

- When one of the synchronisation pulses is missed, the measurement results will become totally uncorrelated. The QBER jumps immediately to 50% (± 1%). The management module should notice this as fast as possible and re-synchronise Alice and Bob by restarting the QKD scripts only.
- Furthermore, the management module monitors the count rates of all eight detectors and the temperature of the crystal. Of course, a failure of one of these components cannot be compensated. The MM can however inform the operator of the QKD link via e-mail about these failures[15].

6.5.4. Hands-off Plug&Play Start of the complete QKD System

The combination of the modules in the previous chapter with the MM allows us to achieve a complete hands-off plug&play operation of the QKD system. Figure 6.17 shows the coincidence rate of the vertical detector and the QBER during a start-up process after the complete system was moved from the Siemens locations to the Austrian Research Centers. One can see that the complete system was automatically aligned and started to produce keys after 22 min without any manual intervention. Note that it took much longer to connect all cables, start the computers etc.

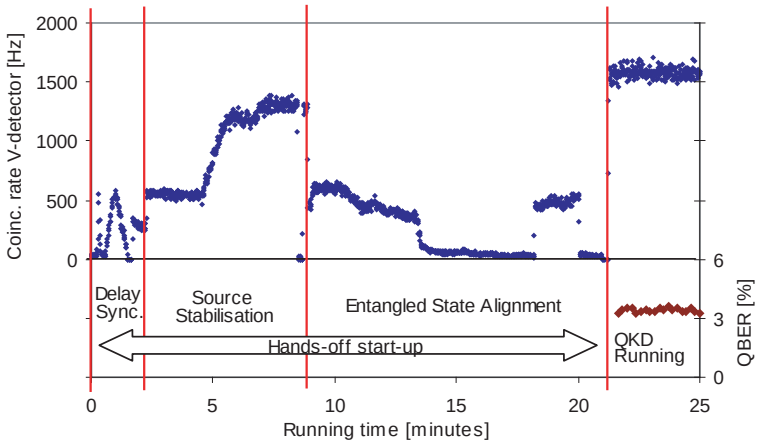

Figure 6.17.: Hands-off start-up process after the QKD system has been transported through Vienna (from Siemens to the Austrian Research Centers). The modules described above (FindDelay, FindWindow, SourceStab, StateAlign) completely align the whole QKD system. The first keys are generated after about 22 minutes. A normal startup (no transportation) takes about 12-15 minutes. One can see that the coincidence rate at the end of the complete startup is higher than after source stabilisation. This is because of the warm-up time of the pump laser and the crystal temperature controller for the entanglement source. Note that this phase takes almost as long as the startup of the QKD system!

[15]For this purpose, the QKD Monitor software includes an interface which allows to send automated e-mails

7. Laboratory Measurements

This chapter presents several experimental results from the laboratory and the first field trials in the Siemens network before the system has been integrated into the SECOQC network.

7.1. Pump power

After the entanglement source is integrated into the final 19" case, it is not possible to access it any more. We therefore made several measurements (using optical fibres) with various pump power settings to find the optimum value. The result can be seen in figure 7.1. The overall coincidence probability (ratio between count rate on Alice and coincidence rate on Bob) is about 4% and stays constant.

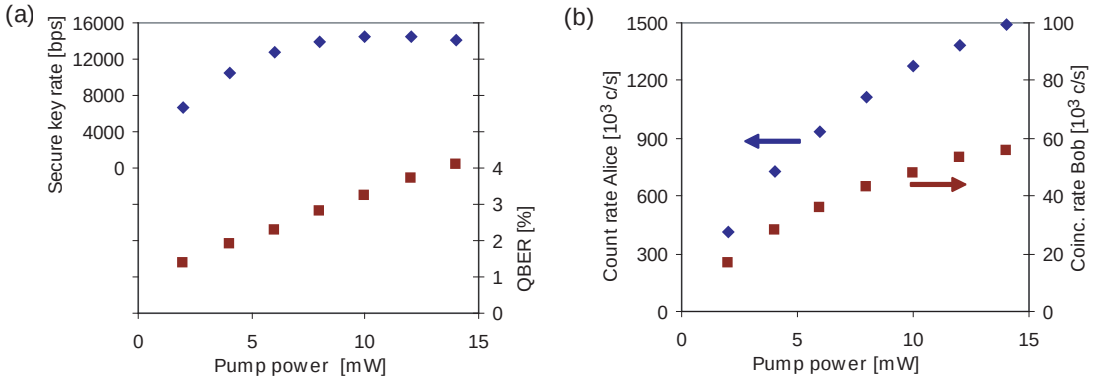

Figure 7.1.: (a) Key rate and QBER at various pump power settings. (b) Alice's count rate (sum of all four detectors) and Bob's coincidence rate at various pump power settings.

From figure 7.1, one can also see that the key rate first increases with the pump power, has a maximum at about 10mW and finally decreases for higher power. This behaviour has two reasons: first, the count rates do not increase linearly with the pump power but show a saturation behaviour. This is because of the hold-off times of the detectors which is necessary to reduce the so-called afterpulsing effect. This is a detection event caused by a trapped charge carrier that is released later and causes a new avalanche. The second reason is the rising QBER which is linearly increasing with the pump power. The reason for this particular behaviour will be discussed in the next section. Because of the error correction protocol and privacy amplification process, any increase of the QBER will automatically reduce the size of the secure key. One therefore has to find a compromise between a high key rate and a low QBER which will rise

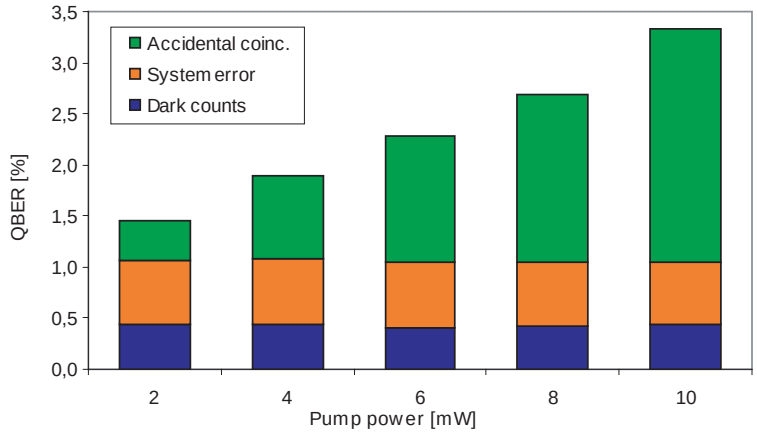

Figure 7.2.: Decomposition of the QBER for several pump power settings into three components: accidental coincidences (multi-pair emission), system errors (optical imperfections) and dark counts.

with longer distances. We decided to set the pump power to 6mW when the system is integrated into the 19"-case.

7.2. QBER Decomposition

In a practical QKD system, some errors will occur even when no eavesdropper is present. We can distinguish four error sources for our entanglement based system:

- Detector dark counts
- Accidental coincidences due to muti-pair emission
- System errors (other errors covering imperfections in the optical elements such as beam splitters and purity of the entangled state)
- Polarisation drifts

To obtain the relative percentage of the various sources, we first measured the dark count and accidental coincidence rates for each detector. The dark count rate can be obtained by blocking the detectors input. Adding some delay in the trigger path allows to measure the background noise that consists of accidental coincidences and dark counts. The accidental coincidences are caused by multi-pair emission during the spontaneous down conversion process [30]. All measurements were made immediately after the state has been aligned carefully to rule out errors due to polarisation drifts and hence this error source was considered negligible.

During the laboratory tests, the QKD software for Alice and Bob was running on a central computer. Additional software allowed to analyse the coincidences after sifting, i.e. to obtain the coincidence matrix. By subtracting the dark counts from the original matrix one can estimate the QBER due to dark counts. The same can be done to obtain the QBER component due

to accidental coincidences. By subtracting both dark count rate and the accidental coincidence rate, we can obtain the remaining error caused by imperfect optical elements ("System error").

Figure 7.2 shows the result for several pump power settings. The QBER increases linearly with the pump power due to multi-pair emissions from the down-conversion process. The multi-pairs are largely unrelated and give therefore uncorrelated results. Since the multi-pairs grow quadratically with the pump power as opposed to the linear increase of the single pair coincidences, the QBER increases linearly. One can see that the QBER component caused by dark counts (∼0.44%) and imperfections of the optical components ("QBER System", ∼0.63%) are - as expected - independent from the pump power.

7.2.1. Dark counts

As we will see in the next chapter, the dark count rate becomes dominant for long distances. The limiting factor is the ratio between entanglement related coincidences and dark counts. We therefore made several investigations of the dark count rates of our four detectors. We expected that the dark count rate increased linear with the trigger (gating) rate. Our measurements (figure 7.3) confirm this expectation.

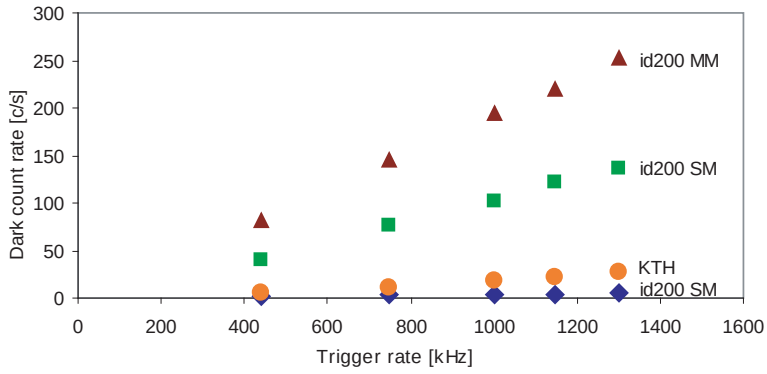

Figure 7.3.: Dark count rates for our detectors for various trigger rates

Table 7.1 summarises some properties of our detectors. Note that all dark count values are obtained after the auxiliary coincidence window which filters about 40% of the dark counts of the KTH detector but has almost no effect on the idQuantique detectors. The KTH detector has very good properties (dark count probability) but requires external water cooling and several power supplies. It is hence not applicable for the SECOQC demonstration where all QKD devices should fit into a 19-inch rack. The KTH detector alone would require a single 19-inch rack. We therefore borrowed a fourth id200 detector for the SECOQC demonstration.

Detector	Gate width	Dark count probability
idQuantique id200 single mode 1	∼1.5ns	$3.9 \cdot 10^{-6}$ per gate
idQuantique id200 single mode 2	∼1.5ns	$1.0 \cdot 10^{-4}$ per gate
idQuantique id200 multi mode	∼1.5ns	$1.9 \cdot 10^{-4}$ per gate
KTH Sweden	∼5ns	$1.8 \cdot 10^{-5}$ per gate

Table 7.1.: Summary of the measured dark count probability for our detectors

7.3. Long distance measurements

The dependency of the key rate on the distance and the maximum distance of the QKD system is inherently interesting. Before we started the measurements, we wanted to know the expected key rate for a certain distance and also the maximum distance. The attenuation of the fibre reduces the coincidence rate and raw key rate. Since the dark count rate is independent of the attenuation, the reduced coincidence rate also effects the ratio between coincidences and noise and hence the QBER. Therefore, the dark count rate of the detectors becomes the dominant factor at long distances.

A simple model allows calculating the expected QBER and key rate for different distances. The attenuation in the fibre reduces the coincidence rate on each detector

$$c(l) = c_0 10^{-\alpha \cdot l/10} \tag{7.1}$$

where c_0 is the average coincidence rate between Alice and Bob at zero distance, α is the attenuation in dB per kilometre of the fibre and l the length of the fibre in km.

In the same way, the accidental coincidences caused by multi pair emission are attenuated

$$a(l) = a_0 10^{-\alpha \cdot l/10} \tag{7.2}$$

where a_0 is the accidental coincidence rate at zero distance.

The total coincidence rate therefore is $4c(l)$ and the total background rate is $4a(l) + 4d$ where d is the average dark count rate per InGaAs detector.

The QBER is defined as:

$$e = \frac{n_{false}}{n_{true} + n_{false}} \tag{7.3}$$

After sifting, the true bits are given by the half of the coincidence rate ($2c(l)$) and a quarter of the total background rate ($a(l) + d$). The false bits are given by just a quarter of the total background rate ($a(l) + d$). The length dependent QBER caused by background coincidences (dark counts and accidental coincidences) therefore results in

$$e_{noise}(l) = \frac{n_{false}}{n_{true} + n_{false}} \tag{7.4}$$

$$= \frac{a(l) + d}{2c(l) + 2d + 2a(l)} \tag{7.5}$$

To consider the imperfections in the optical setup ("system errors"), we add another QBER component $e_{system} \approx 0.65\%$ (the value is obtained from the measurements in the previous subchapter). The complete QBER is therefore:

$$e(l) = e_{noise}(l) + e_{system} \tag{7.6}$$

The final key rate can be calculated with eqn. 4.6 for the number of secure bits $n_{secure}(e)$, including the error dependent overhead for the CASCADE error correction.

$$k_{sec}(l) = \frac{n_{secure}(e(l))}{n_{sifted}} \cdot \frac{4c(l)}{2} \tag{7.7}$$

$$= \frac{4c(l)}{2}\left[1 - \tau(e) - f(e) \cdot h(e)\right] \tag{7.8}$$

The factor $\frac{n_{secure}(e(l))}{n_{sifted}}$ gives the number of secure bits per sifted bit where $(4\ \frac{c(l)}{2})$ is the overall sifting rate.

Figure 7.4 shows the expected key rate compared to experimental results (at 0km, 25km, 50km). It also shows a prediction for an average dark count rate of about 4 Hz which corresponds to the value of our best InGaAs detector (id200 SM1, see table 7.1). During all measurements, the pump power was set to about 6mW with a single count rate on Alice (which is equal to the trigger rate) of about 950 kHz. The other parameters for the model are: $\alpha = 0.2db/km$, $c_0 = 9kHz$ and $a_0 = 240Hz$.

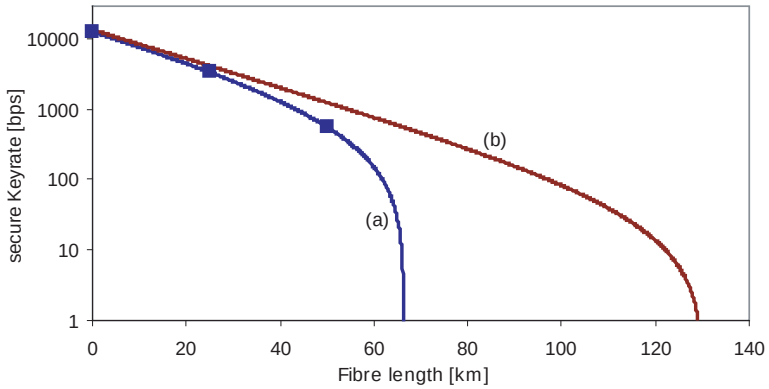

Figure 7.4.: The expected key rate for an average dark count rate of 80 Hz (a) and the experimental values (blue squares). (b) shows the expected key rate for an average dark count rate of 4 Hz, which corresponds to our best InGaAs detector

One can see from figure 7.4 and table 7.2 that the measurements perfectly match the predictions made by the simple model given above. The large average dark count rate (80Hz) of the different detectors we use does not allow a key generation after 65km. An almost twice longer maximum distance is technically feasible. If we assume to have four detectors with the same dark count

Distance [km]	QBER (Model)	QBER (Measured)	Key rate (Model)	Key rate (Measured)
0	2.3	2.3	12494	12500
25	3.2	3.3	3306	3300
50	5.9	6.0	554	550
75	13.0	13.2	0	0

Table 7.2.: Comparison of the values (QBER, key rate) as expected from the model and experimental results

rate as the best detector we have now (4 Hz, id200 SM1), we can reach distances beyond 100km. The predicted key rate at 100km is approximately 90 bps.

Note that the entanglement source has already been used to distribute entangled photons over 100km [35]. The results herein were obtained with the detector with the lowest dark count rate. The problem is that QKD requires four detectors and several optical components (BB84 modules, WDM, PolCtrl) adding further attenuation.

7.4. First long term measurements

In April 2008, we made the first long-term measurements with the QKD system. All measurements presented on the next pages were carried out with SourceStab (sec. 6.1) and PolCtrl (sec. 6.3) only. The other stabilisation and automation modules were conceived because of the experiences during the following measurements. Figure 7.5 shows key rate and QBER for a 12h run with a 25km fibre spool (non-zero dispersion shifted) in the laboratory.

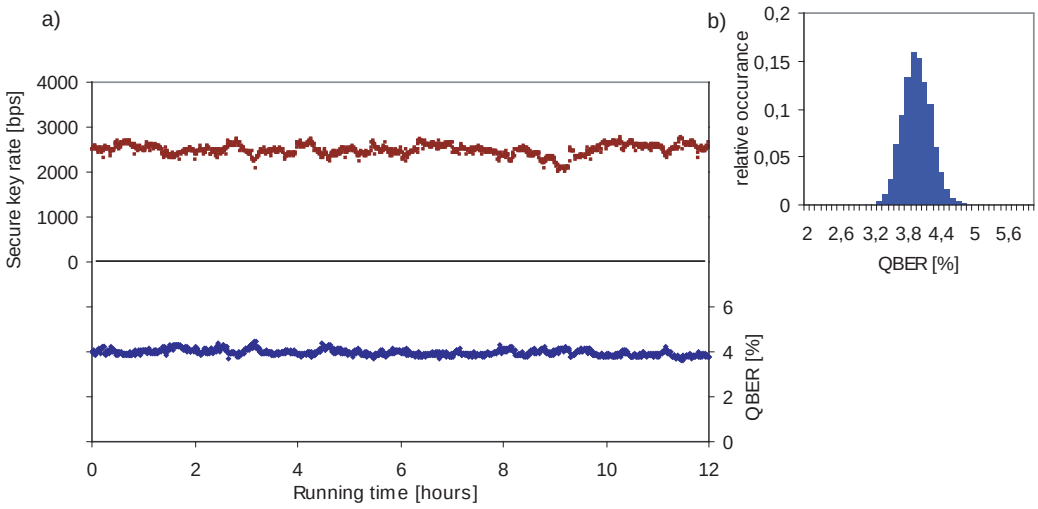

Figure 7.5.: Results of a 12h trial in laboratory environment. (a) Keyrate and QBER (b) QBER distribution (The FWHM of the QBER is ∼0.6%)

7.5. First field trials in the Siemens network

The results in the laboratory environment were very promising. The first measurements outside the laboratory were carried out at an office in Erdberg (ERD). From there, two fibre loops routed via two other Siemens-locations Siemensstrasse (SIE) and Gudrunstrasse (GUD) were accessible (see figure 8.3 for the geographical layout of the locations and fibres).

- ERD-GUD-ERD: 5dB, 12km
- ERD-SIE-ERD: 8dB, 32km

Figure 7.6 shows the results (key rate and QBER) obtained over 24 hours. Note that only SourceStab and PolCtrl were available during the trial.

During the measurements, we noticed several other important influences:

- The complete QKD system (Alice, Bob, detectors, monitoring computer and database server) produces a lot of heat that leads to room temperatures up to 35°C when no air

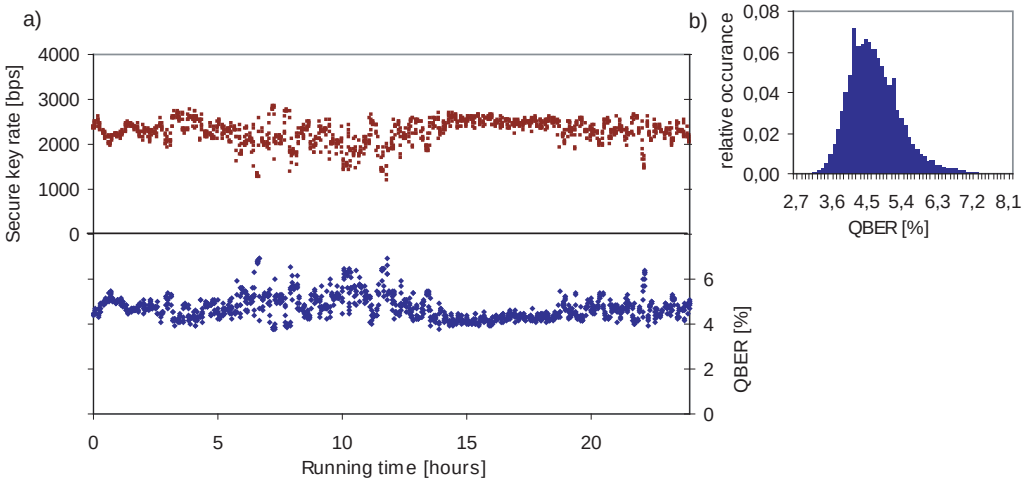

Figure 7.6.: Results of a 24h trial with the deployed ERD-GUD-ERD fibre. See figure 8.3 for an geographical outline of the fibre. The FWHM of the QBER distribution is 1.2%

conditioning is available. At some temperature (∼30°C) the detectors will automatically shutdown.

- Opening the window helps to lower the temperature. However, every temperature change immediately affects the runtime of the electronic pulses in Alice and Bob leading to lower coincidence rate due to the mismatch of the detector gates in respect of the arrival of the single photons. Every reduction of the coincidence rate also increase the QBER because of the lower ratio between coincidences and dark counts and hence strongly reduces the key rate. We therefore needed a reliable module for periodic detector synchronisation (FindDelay, see section 6.4.1).
- Before the measurement, the state had to be aligned manually. Since it was our goal to achieve a complete hands-off operation of the QKD system, we had to conceive the automatic state alignment module (StateAlign, see section 6.2).
- From the rather large temporal fluctuations of the QBER, one can conclude that the polarisation stabilisation module (PolCtrl) was not able to compensate every drift in the complete QKD system (see 6.2.5). With the automatic state (re-) alignment, we are confident to keep the environmental fluctuation of the QBER lower than 1%.

For the long link (ERD-SIE-ERD), the chromatic dispersion (∼20ps/km/nm) becomes dominant. The broadening of the time distribution of the photons (bandwidth ∼3nm) to $\Delta t \approx 2ns$ leads to further losses because of the rather small gate width of the detectors (∼1.5 ns). For a short test (30min) we could obtain a key rate of about 450 bps with a QBER of about 7.5%.

8. The SECOQC Quantum Cryptography Network in Vienna

The previous chapters described the details of our QKD system based on entangled photons. As every other QKD system, it has two major drawbacks:

- A QKD system provides only a point-to-point link
- A QKD link is intrinsically limited in distance

Both disadvantages make it difficult to straightforwardly build a practical quantum cryptography network. The goal of the European FP6-project SECOQC (secure communication based on quantum cryptography) [2] was to build such a network structure. The first prototype has been demonstrated in October 2008 in the fibre network of Siemens Vienna, a typical Metropolitan Area Network (MAN). The prototype includes 8 different QKD links - among of them our system based on entanglement.

This chapter will give an overview of the architecture of the quantum network in Vienna, the integration of our QKD system to the network and the results we have obtained during the test phase in October 2008.

8.1. Architecture of the SECOQC network

A prototype of a simple network structure based on optical switching has been presented 2003 [40] in Boston, USA. This structure allowed to distribute keys between many clients but not to exceed the distance limitation. A quantum repeater network [41] is a possibility to overcome the distance limitation but not yet technological feasible. Other QKD networks based on the same approach as the network in Vienna also have been demonstrated in China [42] and south Durban, South Africa [43] on a much smaller scale.

The SECOQC approach is based on trusted nodes and provides the infrastructure for a key distribution network ("network of secrets") and encryption of user-data. The architecture of the SECOQC quantum network is structured in three layers [44]:

QKD links: Several point-to-point QKD links build the so-called Quantum Back Bone (QBB) network. The links can form any topology like a star, ring, chain or meshed structure as shown in figure 8.1. Each QKD device is located in a QBB node that is considered to be trusted, i.e. to be placed at a secure site. The node is the central element in the network architecture. The

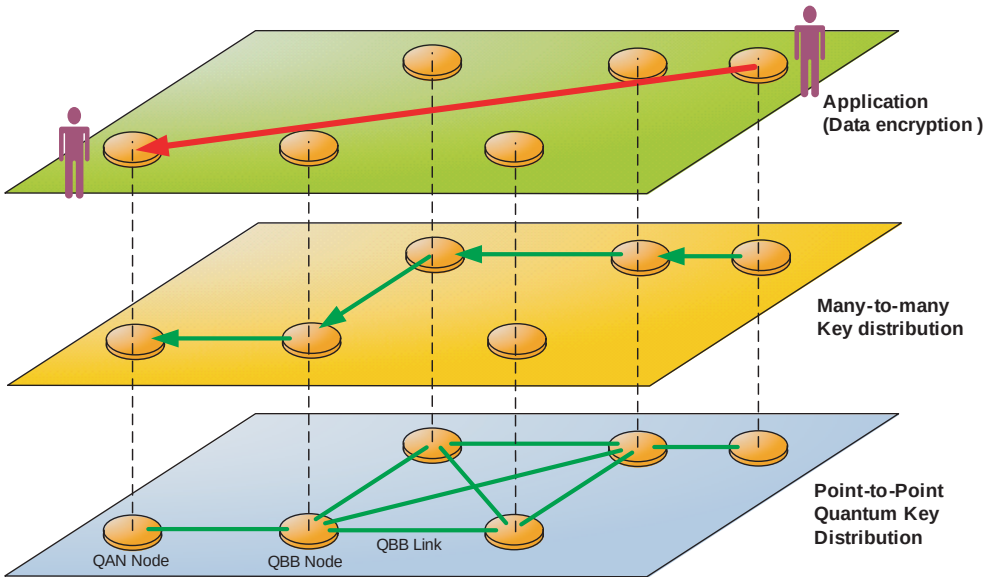

Figure 8.1.: The three-layer architecture of the SECOQC network.

QKD links establish secure keys on a point-to-point basis and pass them to the nodes where the keys are stored. A single-ended node is usually referred to as a Quantum Access Network (QAN) node.

Many-to-many Key Distribution: The main feature of the SECOQC network is the possibility to distribute the keys to non-adjacent nodes in a hop-by-hop scheme. The flexibility of a meshed QBB network allows several other benefits like alternative routes to increase the reliability of the network and parallel operation to increase the overall key rate. All the features of the SECOQC network in Vienna have been demonstrated during the conference and will be discussed later in details.

Key Usage (Data Encryption): The distributed keys between two nodes (adjacent or not) can be used to encrypt data. For this purpose each node provides interfaces (AES or OTP) to encrypt and transmit data between to clients that are connected to the nodes.

8.2. Outline of the Vienna Network

The prototype network [3] consists of 6 nodes and 8 QKD links (figure 8.2 and 8.3). The 6 nodes are located at Siemens offices: SIE (Siemensstraße), ERD (Erdbergerlände), GUD (Gudrunstraße), BREIT (Breitenfurterstraße), STP (St. Pölten), FORUM (Siemens Forum). The four nodes SIE, ERD, GUD and BREIT are so-called QBB (Quantum Back Bone) nodes while STP and FORUM are QAN (Quantum Access Network) nodes. Each node is connected by two standard fibres that are laid out in the underground of Vienna and provided by Siemens Austria. One fibre acts as the quantum channel, the other one as the classical channel. Each node provides an interface for the QKD links to access the classical channel.

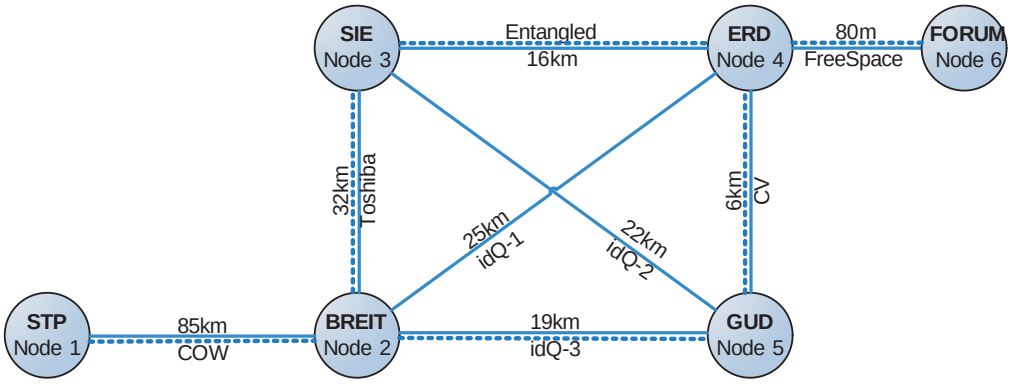

Figure 8.2.: Outline of the SECOQC quantum cryptography network in Vienna. The eight QKD links (table 8.1) come from five different SECOQC-partners (Universities and companies). Each pair is connected with a standard telecom-fiber for the quantum channel (solid lines). Another fibre (dashed) connects the nodes to supply the classical channel.

Link	Distance	Supplier	Technology
SIE-ERD	16km	University of Vienna	Entangled Photons
ERD-GUD	6km	Institut d'Optique Paris	Continuous variables
SIE-BREIT	32km	Toshiba	One way weak pulse system
SIE-GUD	22km	idQuantique	Autocompensating plug&play
ERD-FORUM	80m	LMU Munich	Weak pulse free space
BREIT-GUD	19km	idQuantique	Autocompensating plug&play
BREIT-ERD	25km	idQuantique	Autocompensating plug&play
BREIT-STP	85km	University of Geneva	Coherent one way

Table 8.1.: QKD links for the SECOQC network in Vienna. Details on the other system can be found on the SECOQC website [2]

8.2.1. Demonstration of the quantum network

During summer 2008, a test network has been build up in a laboratory at ARC (Austrian Research Centers). During this time, all QKD systems were integrated to the network nodes. Section 8.3 will describe how this is done for our entanglement based system. After testing the infrastructure, the whole network has been deployed to the Siemens locations in September. This section gives a short overview of the network's features that have been demonstrated during the SECOQC conference (8th - 10th October 2008).

Many-to-Many Key Distribution: For example, a client at the Siemens Forum wants to send some important data to the Siemens headquarter in Siemensstrasse (SIE). For this purpose, both nodes (SIE and FORUM) need the same key. The SECOQC network provides the infrastructure to distribute keys in a many-to-many basis. This is done in a hop-by-hop scheme (fig. 8.4). In the same manner, the chain can be extended in an information theoretical way. Note that the complete chain is only secure if and only if all intermediate nodes are secure.

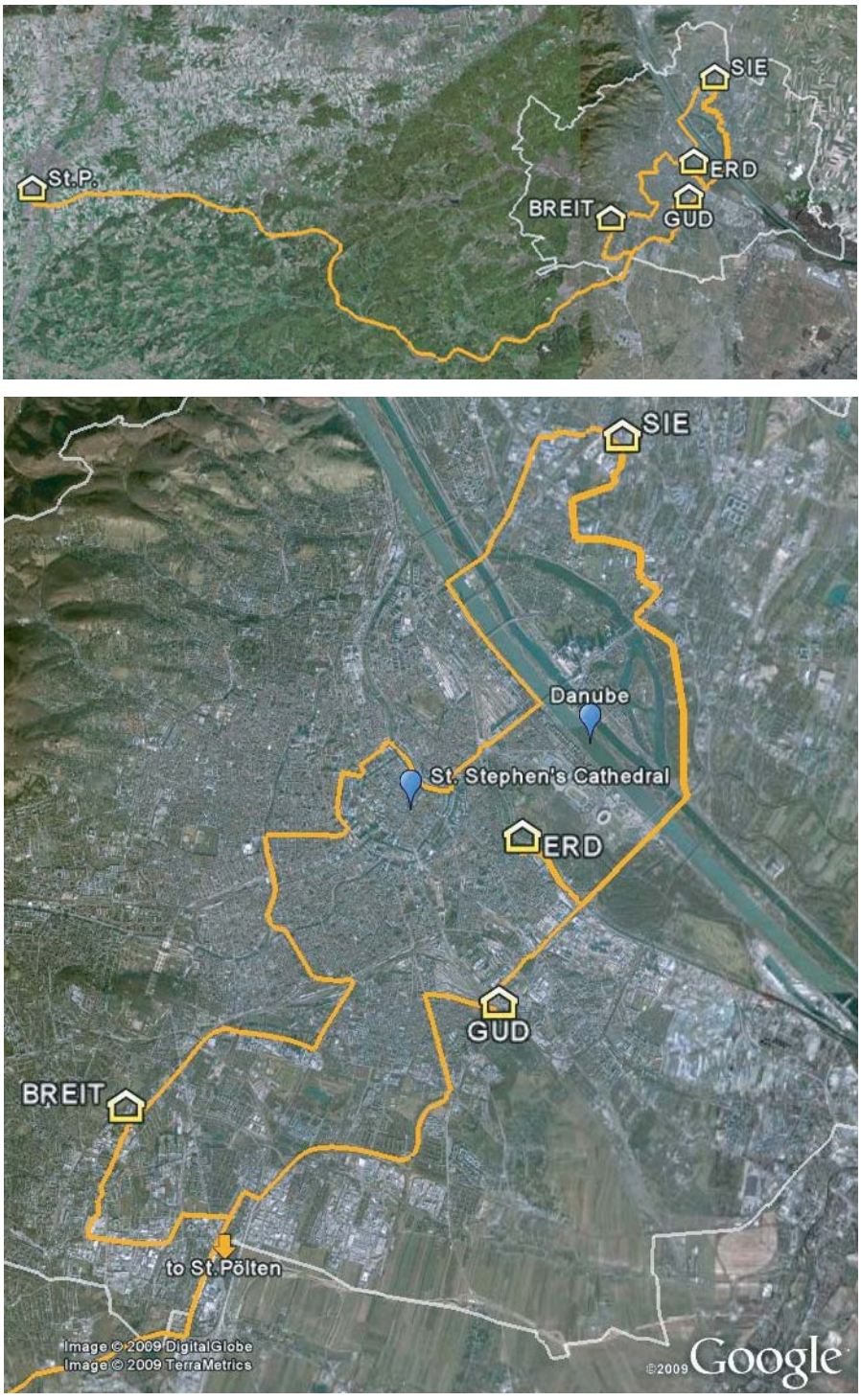

Figure 8.3.: Map of the node-locations and fibres for the SECOQC network in Vienna. The Siemens Forum (FORUM) is close to location ERD (100m). The thicker line corresponds to our QKD link between SIE and ERD. It crosses the river Danube and partially runs parallel to the highway with the highest traffic in Austria. Satellite images taken from Google Earth.

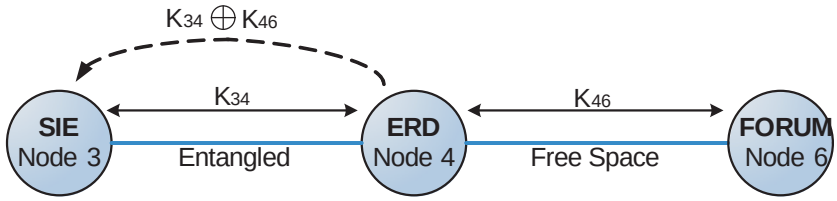

Figure 8.4.: Scheme for the hop-by-hop distribution of keys. Two QKD links provide the point-to-point keys (K_{34} and K_{46}). The node in the middle (ERD) encrypts the first key (K_{46}) using one-time-pad (OTP) and K_{34} and sends it to node 3 (SIE). The latter decrypts the payload using K_{34} and obtains K_{46}. Now, the nodes at SIE and FORUM share the same key (K_{46}) which can be used to encrypt the data from the clients.

Alternative routing: An attack on one of the QKD links will force it to reduce the key rate or even stop the key generation. Say the key store between two nodes (adjacent or not) is exhausted. The meshed structure of the quantum network in Vienna allows to distributed keys even in this case - over an alternative route. Exactly this scenario was demonstrated during the SECOQC conference. We simulated an attack on our QKD link using a heavily attenuated laser at 1550nm[1] that is coupled to the quantum channel with a fibre beam splitter. The OTP-encrypted telephone call from FORUM to SIE (via ERD) was continued until the key storage of the SIE-ERD link has been exhausted. Subsequently, the key has been distributed on the alternative route FORUM-ERD-BREIT-SIE.

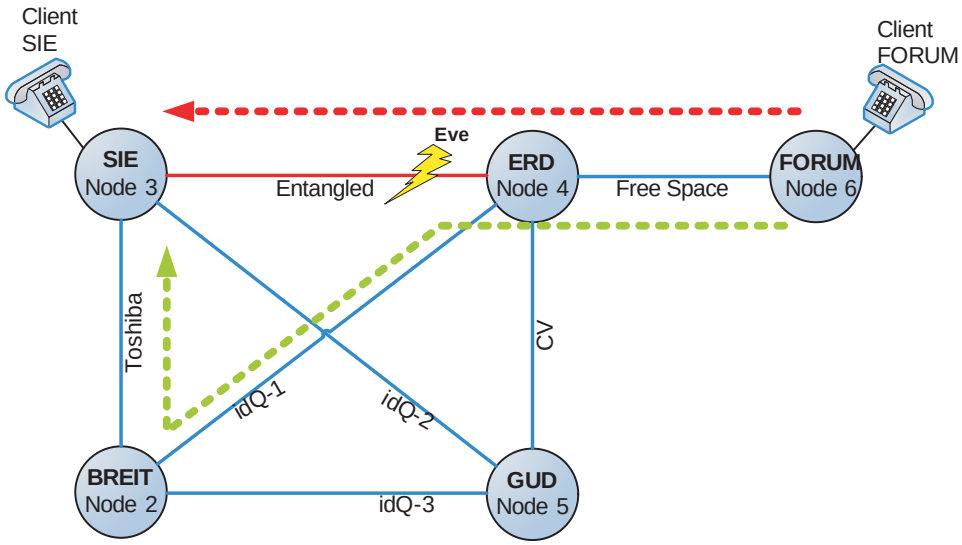

Figure 8.5.: (color) The direct path from FORUM to SIE becomes insecure due to an attack on the entangled QKD system. The meshed structure of the network allows to choose a different path, i.e. the key will be distributed via node BREIT.

[1] Clearly, this is probably the worst attack since no real information was extracted. However, the idea was to simulate a classical amplifier that introduces some noise in the quantum channel.

8.3. Integration of the entangled QKD system to the network

The laboratory prototype of our QKD system was not directly compatible to the SECOQC architecture. To integrate the system into the SECOQC network, we had to make several changes. For example, the QKD stack was running on a single computer. This is practicable but however unacceptable for the SECOQC demonstration, furthermore it is insecure to send the raw measurement results over the network. Due to the low performance of the CPU (PPC405 at 300Mhz) on the Xilinx boards it is not possible to run the QKD post processing stack directly on Alice and Bob [37]. We therefore decided to put the QKD stack on a virtual machine on the node computers. The management module which coordinates the complete QKD system also runs on the node computer. A standardised interface called QBB Link Interface [2] is used to build up the connection to the actual node module mode which contains the key store.

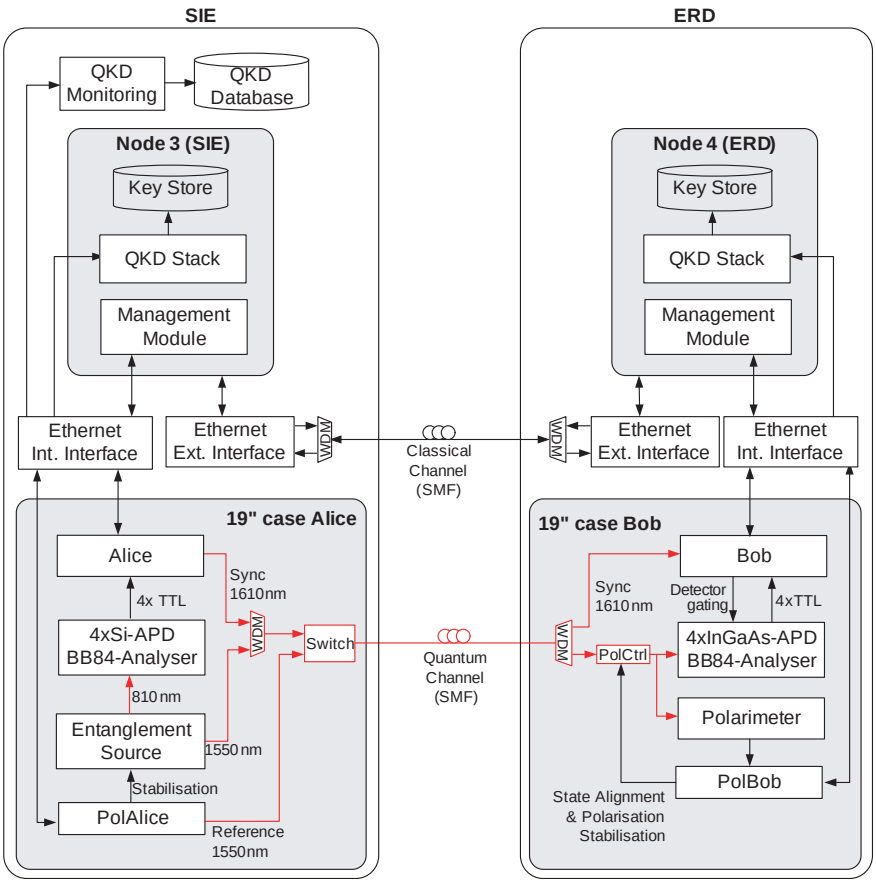

Figure 8.6.: Overview of the QKD system as it was integrated into the SECOQC network. Management module and the QKD protocol stack are placed in the node modules. The nodes are connected using SFP (small form-factor pluggable) modules including a WDM (wavelength division multiplexer) for bidirectional classical communication.

8.3.1. Q3P Tunneling

Apart from the communication over the quantum channel, the complete QKD system requires a lot of classical communication (see figure 8.7): the classical parts of the BB84 protocol, the stabilisation and automation modules (chapter 6) and the monitoring software (appendix A).

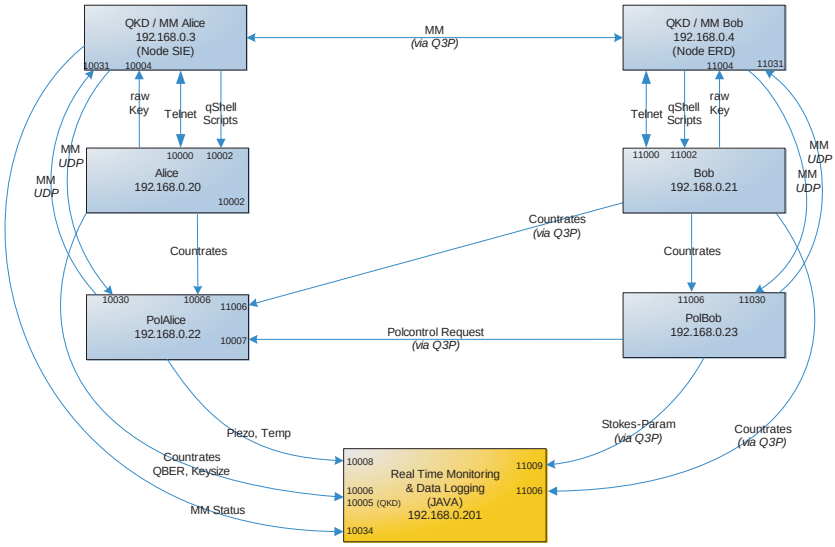

Figure 8.7.: Overview of the communication scheme for the complete QKD system showing IP addresses and UDP ports. Note that the QKD Monitoring software (see sec. A.1) is placed at Alice's location (SIE) during the SECOQC demonstration

.

In the SECOQC architecture, a proprietary protocol called Q3P [45] (quantum point-to-point protocol) is used for the classical communication between the two devices forming the QKD link. Q3P provides plain, authenticated or encrypted communication on a point-to-point basis. A direct connection between the QKD devices (e.g. from PolBob to PolAlice via TCP or UDP) is not available. Every communication between the locations has to be carried out trough the Q3P instance. To solve this problem, every classical communication in our system is tunnelled trough the Q3P channel via the management module that forwards the message to the receiver (see fig. 8.8).

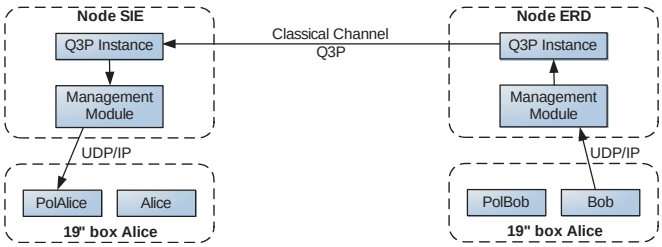

Figure 8.8.: (color) Scheme of the Q3P tunnelling for the classical communication between Alice and Bob. In the example above, Bob sends his count rates to PolAlice (used for SourceStab). The MM on Bob's side receives the message and forwards it to the MM on Alice's side.

8.3.2. Final Node Setup

Figure 8.9 shows the two racks containing the nodes SIE and ERD. Our Alice is placed in SIE and Bob in ERD. Each QKD device is connected to the internal interface of the node using an Ethernet switch. Another switch with single mode fibre SFP modules is used to connect the external node interfaces. This also provides the classical channel for the QKD devices. The racks were placed in ordinary offices without air-conditioning.

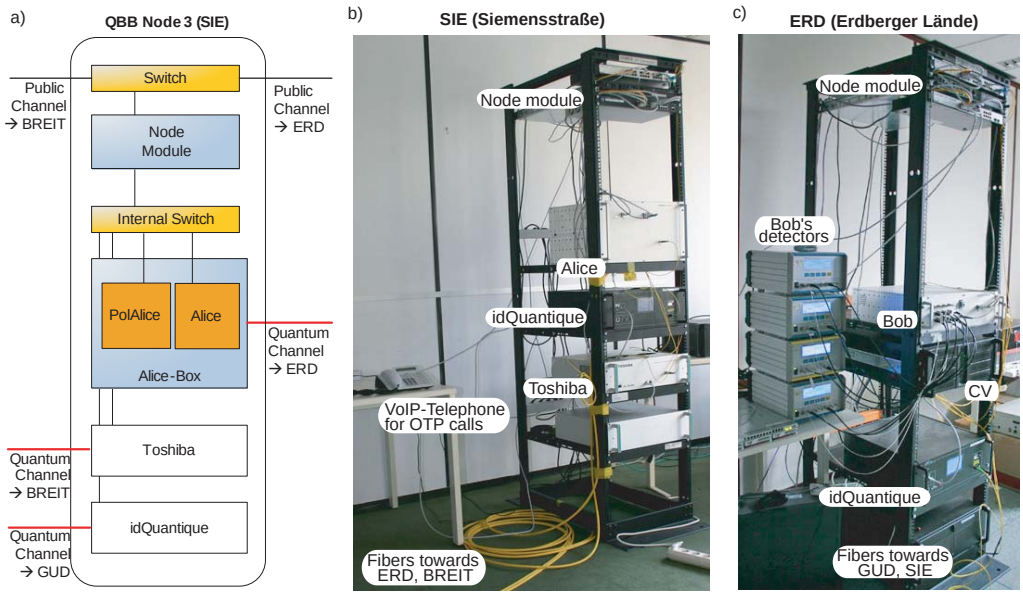

Figure 8.9.: (a) schematic outline of the node in Siemensstrasse (SIE). The QKD devices are connected to the internal node interface. The nodes themselves and the clients are connected to the external (public) interface.
(b) photo of the actual node in SIE. All components (QKD devices, switches, node module) are in installed in a 19-inch rack. The voice-over-IP telephone is used to make OTP encrypted calls to any other node.
(c) node at ERD containing Bob. Only the four id200 detectors are placed outside the rack (because of a missing platform for the 19-inch rack in ERD).

8.4. Results during the two-week SECOQC demonstration

This section presents the major results we obtained during the two week demonstration in the SECOQC network from Oct. 8th (first day of the conference) until Oct. 22nd. It must be stressed that all results presented here were obtained without any manual intervention to the QKD system.

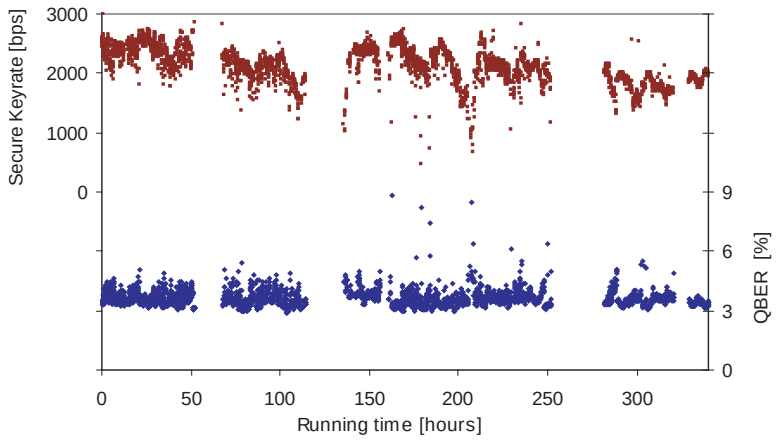

Figure 8.10.: Final secure key rate and QBER during the two-week demonstration of the SECOQC network.

Figure 8.10 shows key rate and QBER during the two-weeks demonstration. One can identify three major facts that will be discussed in detail within this section

- The QBER has been very stable between 3.0% and 4.5% with an average value of 3.5%.
- The key rate shows a slight decrease from 2500 bps to 2000 bps. One can also see a large fluctuation in the key-rate. Both is caused by a problem with the long-term stability (temperature dependency) of the id200 detectors (see sec. 8.4.1). The overall average lies at about 2100 bps.
- There are several gaps, i.e. interruptions of the QKD process including three longer ones. These are caused primarily by problems in the classical parts of the network (see sec. 8.4.2)

Figure 8.11 shows the entanglement visibility (defined as $V = \frac{max-min}{max+min}$ where max is the maximal coincidence rate for orthogonal polariser settings and min the minimal coincidence rate for parallel polariser settings) and temperature in the office where node ERD was located.

The average visibility is about 93%. A confidence level of 99.9% to obtain a visibility higher than 90% is achieved. Very low values (<90%) are caused by strong mechanical changes of the fibre during work in the node-rooms. The temperature has been measured in the node room ERD and is caused by the open window. This was the only way to keep the temperature in the room low. The situation also applies for the other node room in SIE (Alice).

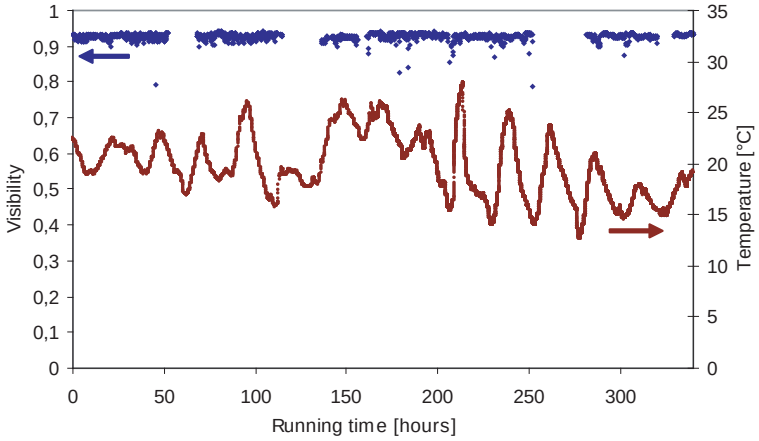

Figure 8.11.: Visibility and temperature during the two weeks demonstration. One can see that the system manages automatically to keep the entanglement stable on a high visibility despite the high temperature fluctuations in the office ERD where Bob was installed.

Figure 8.12 show key rate and QBER during the first 48 hours. One can see a periodic temporal drift in the QBER. We expected this behaviour as a result of heavily temperature fluctuations in the room. As intended, the management module starts a re-alignment of the entangled state when QBER rises above a threshold value (initial QBER + 1%).

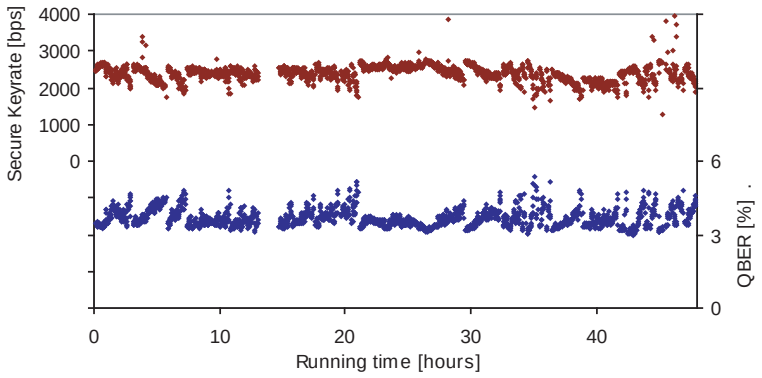

Figure 8.12.: Final key rate and QBER during the first 48h of the demonstration.

Figure 8.13 shows the correlation between QBER drifts and temperature fluctuations. The large temperature fluctuations in the node rooms cause a drift of the polarisation that cannot be compensated by PolCtrl (see section 6.2.5). Strong temperature changes will immediately lead to drifts in the QBER while a constant temperature (e.g. between hours 7 to 13 and 22 to 28) also keeps the QBER stable.

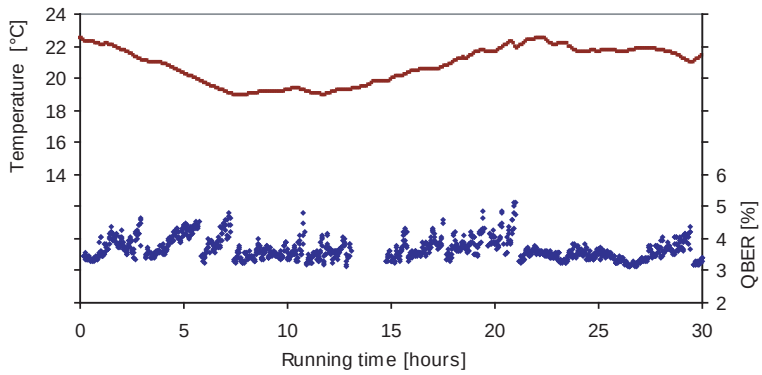

Figure 8.13.: (color) QBER and temperature measured inside the ERD node room during the first 30h.

Figure 8.14 compares the QBER distributions during the complete two week demonstration (336h) and a typical 12h-run under laboratory conditions. The temperature-induced polarisation drifts lead to a slight asymmetry in the 336h-distribution towards higher QBER values. Values above 5% are negligible (probability 0.1%). Note that the FWHM of the QBER distribution is about 0.8% which is very close to the best-case value during tests under laboratory conditions (0.6%). The value is significantly better than the first 24h measurements in the SECOQC network (1.2%, see fig. 7.6) because of the new stabilisation modules. Note also that the QBER distribution in the real-world fibre is the same for the first two days and the complete two weeks period. We therefore believe that a reliable entanglement distribution is possible for even much longer periods than two weeks.

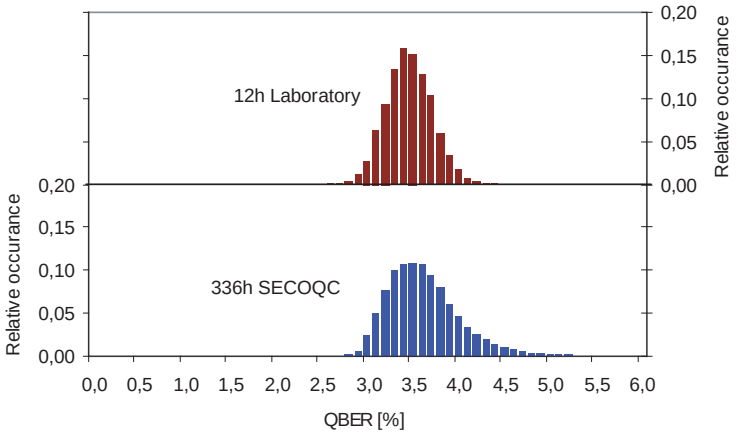

Figure 8.14.: QBER distribution during the complete two-week demonstration (336h) and a typical 12h-run under laboratory conditions.

8.4.1. Long-term stability of the InGaAs detectors

During the two-week demonstration we noticed a strong fluctuation of the coincidence rate that is correlated to the temperature in the node room (see fig. 8.15). One can see that the coincidence rate decreases with low temperatures. We also noticed that the dark count rate decreases proportional. Therefore, we assume that the reduced coincidence rate is caused by a reduced single photon detection efficiency.

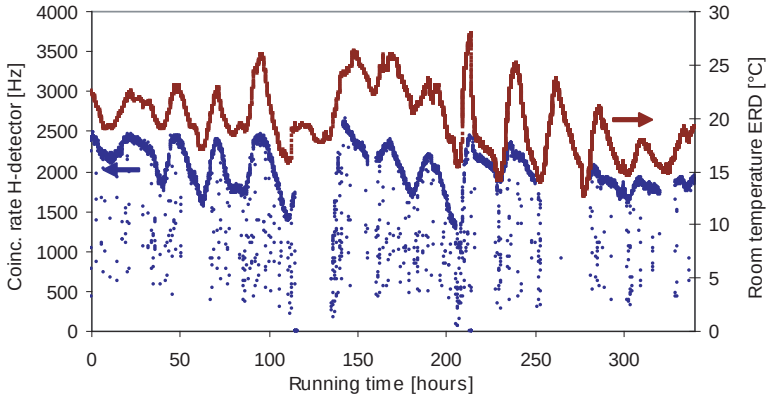

Figure 8.15.: Correlation between the coincidence rate of the id200 detetors and room temperature where the detectors are located (node ERD). The lower rates below the average line are due to the state realignment which is triggered by the large fluctuation of the temperature.

The dilemma is that the window in node room ERD could not be closed because no air conditioning was available. The temperature would immediately rise to more then 30°C which causes the detectors to shutdown. On the other hand, the open window caused the large temperature fluctuation seen in figure 8.15. We have reported the problem to idQuantique where the problem could be reproduced and is further investigated. Note that this problem should not occur in an appropriate environment with air conditioning (a typical server room is kept to a constant temperature of about 22°C $\pm$ 1°).

8.4.2. System availability

In figure 8.10, one can see that there are several gaps in the key generation process. As long as the key rate is higher than the consumption rate, the key store in the nodes can buffer an interruption of the single QKD link. When the buffer is exhausted, an alternative route for key distribution must be taken. For normal data encryption (e.g. video conference), we used AES with a key exchange rate of 4 seconds and a key usage of about 1000 bps. On a two-week average, our QKD link produced about 2100 secure bits per second (when the link is running). Hence, the minimum availability should be 48% to guarantee a seamless key exchange without exhausting the key storage.

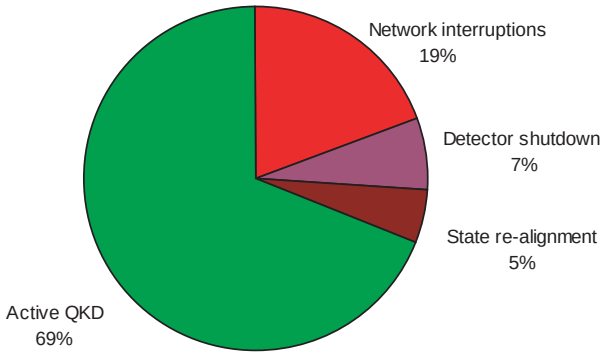

Figure 8.16.: Pie chart showing the proportion of active QKD and interruptions during the two-week SECOQC demonstration.

From fig. 8.16 one can see that we achieved more than the minimum required availability (48%) with an uptime of about 226 hours (67%), despite numerous interruptions:

- Most of the downtime (65 hours, 19%) has been caused by various problems in the classical parts of the prototype-network. This is not surprising since the SECOQC architecture is based on proprietary protocols like Q3P [45]. However, it is remarkable that the classical parts of the network caused more down-time than the quantum optical part (65h vs. 17h for state-alignments).
- We decided to shut down the detectors after we recognised a significant decrease in the count rate. Later, we found out that a restart does not help (see previous section) to avoid the temperature dependency of the detection efficiency. A second shutdown has been caused by an increase of the room temperature above 27°C. Both shutdowns led to a total interruption of 22.5 hours (7%).
- The large fluctuation of the temperature causes a rather fast increase of the QBER[2]. On average, the management module therefore had to initiate a re-alignment of the entangled state every 2.5 hours. Every re-alignment takes about 5-10 minutes. In total, the state re-alignments caused a total interruption of 16.6 hours (5%)

[2]Temperature fluctuations in the node room where Bob is installed cause a polarisation drift in the BB84 module that cannot be compensated by PolCtrl, see sec. 6.3.5.

8.5. Use-case scenario: "Long Night of Science"

The so-called "Lange Nacht der Forschung" (long night of science) is a public exhibition that took place on November 4th. Almost 400 research groups in several locations throughout Austria presented their work.

We presented a complete quantum cryptography system that consists of our entanglement based QKD system and two SECOQC nodes (SIE and ERD, see fig. 8.17). A video conference between two clients was encrypted using AES with a key-exchange interval of 10 seconds (key usage: about 400 bps). The clients (two notebooks with webcams) were placed on different tables and each connected to a node. The ERD client displayed the video from a webcam on top of the SIE client and vice-versa. Alice and Bob were connected by a 25km fibre spool. The QKD Monitor software (A.1) allowed the audience to watch influences on the quantum channel (e.g. shaking the fiber).

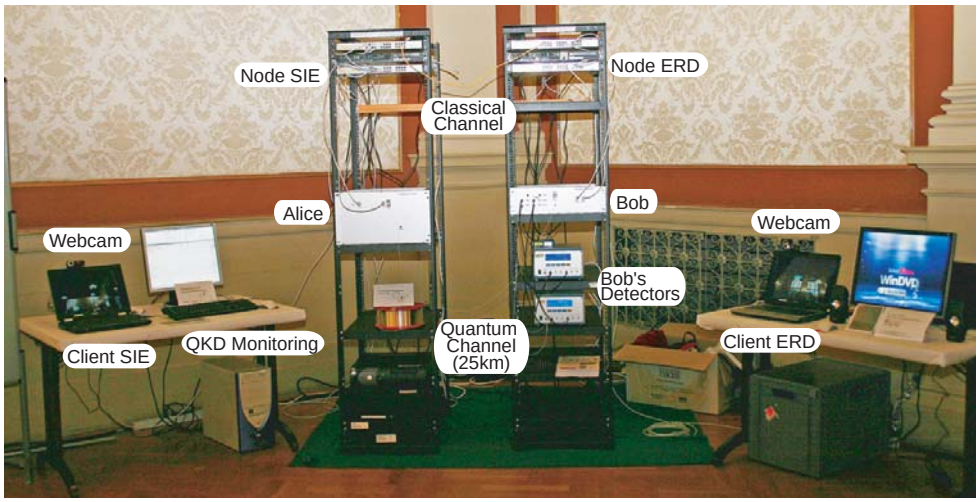

Figure 8.17.: The complete quantum cryptography setup during the "Lange Nacht der Forschung". The nodes encrypt the bidirectional video-stream between the clients. Our QKD system provides the keys over a 25km fibre.

The public interest was enormous. However, the scenario is interesting because of several other reasons: We were able to deploy a complete quantum cryptography system within several hours to a location in Vienna. Transport from the Austrian Research Centers to the main building of the University of Vienna took about 60 minutes. When Alice and Bob are not in the same building, one has to consider at least another hour. To build up the 19"-racks, computers, nodes, QKD devices and connect the various components, about 90 minutes are necessary. Our plug&play QKD system just needs to be connected, starts completely automatically and produces the first keys 20 minutes later (∼1500 bps, 3.2% QBER). Note that only two detectors were used for the public demonstration.

9. Résumé and Outlook

Here, a summary of the achievements in this thesis is given, together with an outlook of further experiments and improvements.

- Fully automated long-term operation of the whole QKD system which is compatible with standard 19-inch racks
- Stable hands-off entanglement distribution in an inner-city laid-out fibre even in worst-case conditions with high temperature fluctuations.
- Average visibility of 93% during the two-weeks network demonstration. With a confidence level of 99.9% to have a visibility higher than 90%.
- Reliable key distribution: more than 2kbit/s and 3.5% QBER during the two-week demonstration. The QBER fluctuation (FWHM) was about 0.8%, compared to 0.6% in a laboratory environment.
- The uptime of the QKD link has been about 67% during the demonstration. We expect to achieve system availability of 97% in a standard server-room environment.
- Simple deployment of a complete quantum cryptography system when the QKD system is combined with the SECOQC infrastructure.

As mentioned in the introduction, every QKD system participating in the SECOQC network had to fulfil several criteria regarding key rate, stability and hands-off operation. What makes our system different from the others is that is based on entanglement. Entanglement is a resource also for other quantum information techniques like quantum teleportion, quantum dense coding and quantum computing. Entanglement also plays an important role for QKD issues like device-independent security schemes [46]. We therefore believe that the maturity of entanglement distribution and QKD achieved within this thesis is an important step not just for practical quantum cryptography but also for other quantum information schemes.

Still, there are some possible improvements of the current QKD system and open security issues that are shortly summarised in this chapter.

9.1. Towards a continuous operation of the quantum cryptography system

If we assume that the problems in the classical part of the network can be solved and the nodes are placed in an environment with a stable temperature (e.g. a typical server room), the dominating reasons for an interruption of the QKD can be eliminated.

We are very confident that a stable long-term operation of the complete entanglement-based quantum cryptography system (QKD system + two node modules) is possible. From fig. 8.14 one can see that the QBER distribution is almost the same for 12 hours and 2 weeks. This suggests that a stable entanglement distribution should be possible for longer periods as well.

When Alice and Bob are placed in a temperature stable environment, the average re-alignment period should be increased from 2.5 hours to at least 5 hours. Hence, a hands-off and stable key generation with an average uptime of about 97% is achievable without any further changes to the QKD system.

9.2. Stabilised BB84 module

At the moment, Bob's BB84 module consists of standard fibre components (BS, PBS) that are connected by FC/PC plugs and connection fibres with a length of one metre. Hence, the complete BB84 module becomes very prone to polarisation drifts caused by temperature fluctuations. As pointed out earlier (sec. 6.3.5), this has indeed been a large problem during the network demonstration because of the lack of any air conditioning in the node rooms.

We expect a significant improvement of the polarisation stability with a new, spliced BB84 module with shorter fibre connections that is furthermore mounted on a temperature stabilised (e.g.using peltier elements) plate .

A different stabilisation approach - based solely on the QBER - is presented in the next section. This approach should be able to compensate every polarisation drift, independent of its origin without disrupting the QKD operation.

9.3. QBER based state stabilisation

The current approach of polarisation stabilisation (PolCtrl, see sec. 6.3) relies on strong reference pulses with a fixed polarisation that are sent from PolAlice and analysed by PolBob. PolCtrl can only compensate drifts in the quantum channel but not in other parts of the system (mainly the fibre-based BB84 module in Bob). Our experiences during the two-week SECOQC trial showed that the latter is dominating. The laid-out fibre itself is rather stable[1].

[1] See for example [7] where several polarisation measurements of the fibre links are shown

A different approach is to use the QBER itself to stabilise the entangled state. In principle, one could use the same approach that SourceStab (sec. 6.1) uses. Two polarisation controllers, one in each basis could be driven consecutively by the hill-climber algorithm to minimise the QBER. The results from the automatic state alignment procedure (sec. 6.2) show that this approach works well and compensates even polarisation drifts that are not compensated by the current PolCtrl. In the current scheme of our system, it is no problem to send the QBER to PolBob. This would not even require an additional Q3P-tunnel.

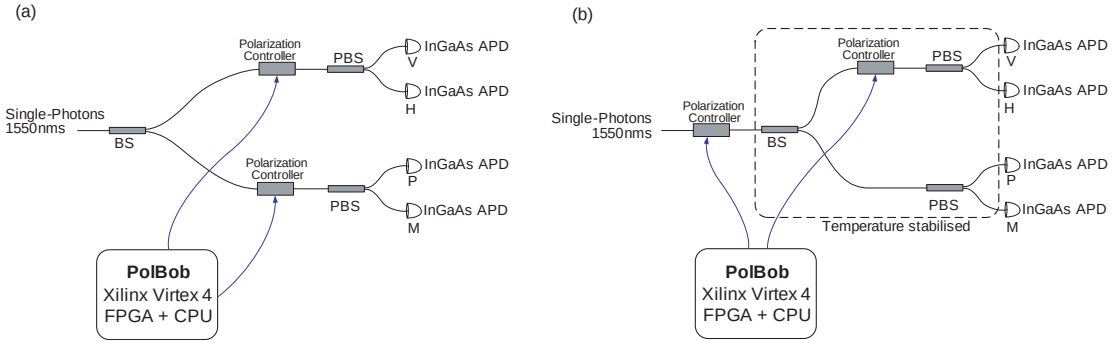

Figure 9.1.: Alternative schemes for a QBER based polarisation control.
(a) in variant 1 a polarisation controller is placed in every arm of the BB84 module to stabilise each measurement basis separately. This approach allows to compensate every drift, even if it occurs in the BB84 module itself.
(b) in variant 2 a temperature stabilised BB84 module is assumed reducing polarisation drifts in the BB84 module. Remaining unavoidable drifts in the quantum channel can be compensated using a single polarisation controller. The second controller is used only for the initial alignment at the system start-up. The advantage of the second variant is that less DAC-channels (degrees of freedom) have to be controlled by PolBob during the control cycle.

The QBER based stabilisation has the further advantage that no auxiliary optics (reference-diodes, fibre-switches and polarimeter) are necessary as shown in fig. 9.1. Additionally, the QKD does not need to be interrupted. As in the case of SourceStab, this approach can run parallel to the QKD operation.

Because of the high statistical fluctuation (FWHM is about 0.6%, see figure 8.14), one would need a long averaging time to obtain a reliable QBER value. Since typical fluctuations in the laid-out fibre are in the range of 2-3 hours, this should not be a problem. We also assume that a temperature stabilised environment for Alice and Bob should reduce the fluctuation in the BB84 module to about 5-6 hours.

The only disadvantage of this scheme is that it is rather slow and cannot directly compensate short term fluctuations like mechanical movement of the fibre. However, our management module has the ability to detect a short-term increase of the QBER and start a re-alignment immediately.

9.4. Side-channel Attacks

Beside theoretical attacks on the BB84 protocols, a completely different class of (technologically feasible) attacks, the so-called side channel attacks exist. Eve tries to take advantage of any information leakage or even tries to actively attack the system exploiting imperfect implementations.

Here, an overview of some side-channel attacks that apply to our QKD system is given. Note that each attack only allows to make some statistical assumptions on the raw key and does not give full knowledge of the complete (raw) key.

9.4.1. Detector efficiency mismatch

An obvious weak point is caused by differences in the efficiency of single photon detectors. This leads to a slightly biased count rate, i.e. more ones than zeros in the raw key. This also applies to our QKD system. The difference in the count rate for the four detectors on Alice's side is about 10%. On Bob's side, the detection efficiency of the InGaAs detectors can be matched by manually changing the bias voltage. Another possibility is to discard a fraction of the counts from detectors with higher efficiency to obtain a equal count rate. Alternatively, a stronger privacy amplification with an estimated information leakage can be used.

9.4.2. Response time mismatch

A different type of side-channel attack makes use of differences in the response times of the detectors[47]. In our case, the four detector modules on Alice's side are susceptible to this problem and introduce a detector dependent delay between the synch-pulse (1610nm) and the single photon (1550nm). Eve could obtain some knowledge by measuring the time between the photon and the trigger pulse (fig. 9.2). The typical difference of the central position if the time-distributions lies around some hundreds picoseconds and hence is resolvable[2].

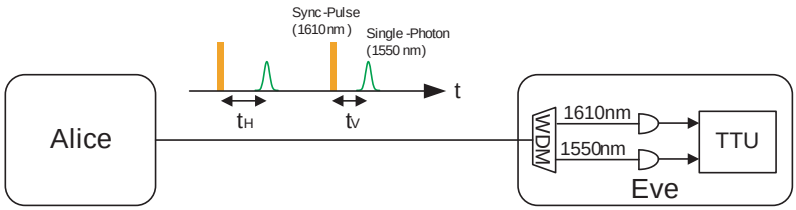

Figure 9.2.: Eve could measure the time between the sync-pulse and the single photon using a time-tagging unit (TTU) to gain knowledge of Alice's measurement result. Without compensation, the time between trigger and photon depends on the different response times of the detectors (e.g. t_V for the vertical detector and t_H for the horizontal detector).

[2] Bob's time-tagging-unit has a resolution of 82ps. However, we also have to assume that Eve has better equipment as it is available now

The individual delay lines on Alice's FPGA board can be used to compensate the different response time of the detectors. This needs to be done manually in the laboratory before the system is deployed. We assume that temperature fluctuations cause the same change in the detector response for every detector. However, this still needs to verified experimentally. If this assumption turns out to be wrong, a similar re-synchronisation module as we have it on Bob's side (FindDelay, see sec. 6.4.1) is necessary.

To verify the correct response-time compensation, we can use Bob's time-tagging unit[3]. When Alice triggers only one detector[4], Bob can measure the time-distribution of the detection event in respect to the trigger. This can be done for every Si-APD detector. Differences in the time distribution indicate a difference in the detector response time. The measurement should be carried out with and without the individual delay lines to measure the original time-distribution and to see if the compensation works correctly. Note that the time distribution must be measured always with the same detector on Bob's side.

9.4.3. Time-shift attack

A similar approach [48] makes use of imperfect synchronisation between the photon and the detector gates. This attack applies to all QKD schemes with gated detectors. Thus also to our system. Eve actively changes the delay between the trigger and the single photons. From fig. 9.3, one can see that such a change (e.g. position A or B) causes a difference in the coincidence rate and hence an efficiency mismatch (9.4.1).

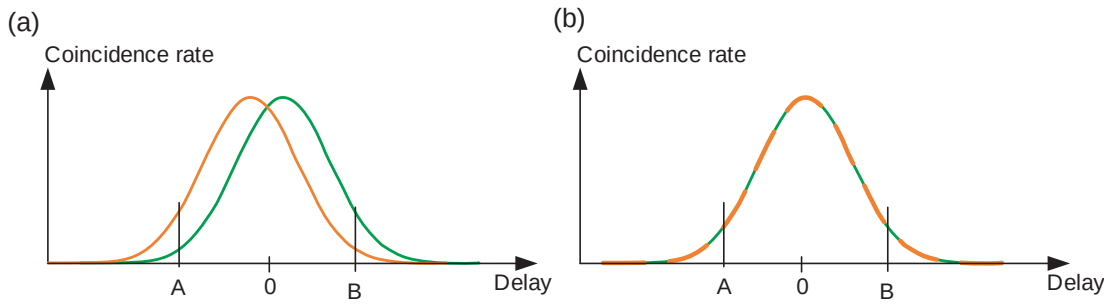

Figure 9.3.: Principal scheme of the time-shift attack.
(a) The green and orange lines show the time-distribution of two detectors in one basis when Eve delays the photon in respect to the detector gate or vice versa.
(b) The time-shift attack is not possible when the time-distribution of both detectors have the same centre position in respect to the trigger pulse.

When Eve chooses a fixed delay (e.g. position A), she might get caught because Alice and Bob could notice the different coincidence rates. In our case, the management module monitors the coincidence rates. When Eve frequently switches between delay A and B, the overall coincidence rate will be the same for both detectors.

[3] that is usually used to set the auxiliary coincidence window, see section 6.4.2
[4] Alice is able to individually enable the detector inputs using the QSH interface.

Note that differences in the gate width are not a problem considering a time-shift attack. From fig. 9.4, one can see that Eve cannot find two delays A, B with different detection efficiency when the detectors are properly synchronised. Only an overall increase of the count rate of one detector occurs which can be recognised easily).

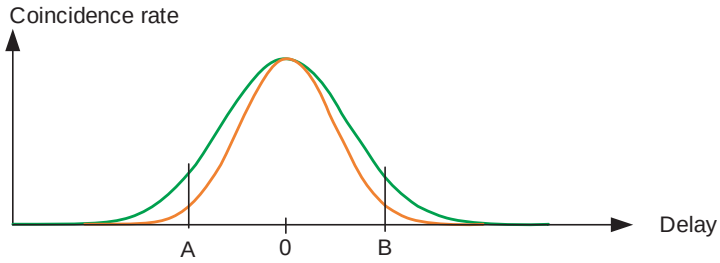

Figure 9.4.: A time-shift attack is not possible when the detectors are synchronised properly even when the gate width is different.

From fig. 6.14, one can see that our detectors in principle have a different internal delay of approx. 500ps (time between incoming trigger-pulse and the actual detection gate). We can use the individual delay (on Bob) to compensate this difference. We believe, that the already incorporated delay-adjustment module (FindDelay, see section 6.4.1) is able to compensate the timing mismatch with the required precision (the maximum timing mismatch must not be higher than the timing jitter). Of course, this needs to be verified experimentally, by testing the side-channel attack on our system.

9.4.4. Implementation of the time-shift attack

A time-shift attack has already been implemented on the commercial idQuantique ID500 QKD system [48]. In our system, the sync/trigger pulses and the single photons are transmited over the quantum channel. Hence, Eve can implement the time-shift attack by delaying the photon in respect to the trigger pulse.

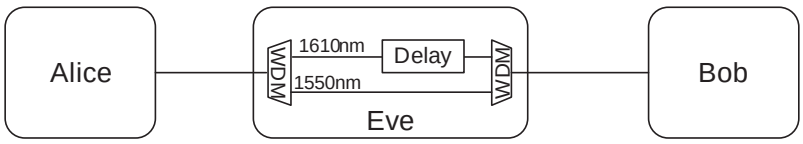

Figure 9.5.: Implementation of a time-shift attack on our QKD system

As mentioned above, we believe, that the precise detector-photon synchronisation protects us from the time-shift attack. We can test this assumption by implementing the attack. Simpler as the implementation in fig. 9.5 is to use the internal delay in the idQuantique id200 detectors. When the delays of all detectors are changed equally, all detector gates are delayed in respect to the trigger pulse. However, such a measurement is not possible at the moment: the management module periodically starts a re-synchronisation and compensates the introduced delay.

9.4.5. Detector saturation loophole

A different approach for a side-channel attack is presented in [49]. There, an error in the circuit of Perkin Elmer Si-APD modules is exploited. A strong light pulse can bring the detector from Geiger mode (which is used to detect single photons) to linear mode (used to detect strong, classical light pulses). By sending such a (non-polarised) pulse, Eve could bring all four detectors in the BB84 module into linear mode. Another pulse with a certain polarisation and a certain power can activate only the detector corresponding to the polarisation of the pulse, i.e. the H-detector will click with certainty if Eve sends a horizontal pulse. This would allow Eve to significantly improve the intercept-resend attack.

This attack has some significance for our system since we use the same type of detector on Alice side. However, Eve has no access to the fibre that connects the source and Alice's BB84 module because the entanglement source and Alice are in the same place.

9.5. Detectors

Telecom-wavelength (1550nm) single photon detectors are a major issue for every quantum communication system. As pointed out in section 7.3, for longer distances towards and beyond 100km, the dark count rate becomes a dominant factor and hence determines the reach of a QKD system. Another important factor is the hold-off time which is necessary to prevent so-called afterpulsing detection events. Such an event is caused by a loosely trapped charge carrier that causes an avalanche at the next gate pulse. The only way to prevent an afterpulsing event is to wait for a certain time. In our case, this hold-off time is set to 10μs for every id200 detector.

Recently, Toshiba presented a very innovative InGaAs detector concept[50] to detect and quench the avalanche much faster than previous quenching circuits. This significantly reduces the after pulsing probability and hence allows faster gating frequencies in the GHz region. Using these detectors, a QKD system with GHz clocking has been presented with a secure key rate of 2.9kbps at 100km [51].

A different approach is pursued by upconversion detectors. Upconversion is the inverse effect of downconversion. The qubit-photon is combined with a strong laser pulse to be converted to shorter wavelengths that can be detected by Si-APDs with high efficiency. In [52], such upconversion detectors were integrated into a QKD system. The detectors had an quantum efficiency of 2.1% a dark count rate of 2.8kHz and a low timing jitter (∼60ps).

Another interesting technologie is the superconducting photon detector (SSPD). In a superconducting nanowire, the energy of a single photon is enough to heat the wire leading to normal conductivity. The difference in the current flow can be measured. Using such detectors and an attenuated laser clocked with 10 GHz, a QKD system over 200km [53] has been presented. The huge disadvantage of the SSPD is the required cryogenic equipment. However, with such detectors we believe that our system can easily reach 100km.

Detector	Max. Clock	Max. count rate	Quantum efficiency	Dark counts	Timing jitter
id200	4MHz	100kHz	10%	$5{\cdot}10^{-5}$/gate	<600ps
Toshiba self-differencing	1.25GHz	100MHz	11%	$2{\cdot}10^{-6}$/gate	55ps
Upconversion	Free running	15MHz	2%	2800 Hz	66ps
SSPD	Free running	1GHz	2%	10Hz	60ps

Table 9.1.: Comparison of available telecom wavelength single-photon detectors. Note that dark count rate for the InGaAs detectors are referred to maximum clock rate. Data taken from [54, 50, 53, 52] and our results with the id200 detectors (see sec. 7.2.1)

A. Real-time Monitoring and Database Logging

During the development of the modules explained in chapter 6 it was absolutely essential to have a real time monitoring solution. Since each module influence several parameters of the QKD system, we needed a comprehensive real-time view on the relevant data: QBER, secure key rate, count rates, status information etc. Furthermore, we needed an efficient method to store the large amounts of data obtained during the long-term measurements combined with comprehensive methods for post-measurement analysis.

At the beginning of 2008, for each device, a separate LabView program was running on a separate computer. Each of them displayed the recent value on a small graph and wrote the value to simple log files. This approach was already very impractical in a laboratory environment, but completely impossible to use when the system is integrated in the SECOQC network where Alice and Bob will be in different locations in Vienna!

In this thesis, a different approach is presented. A completely new solution for monitoring and logging has been developed using components (Java, MySQL) that are a widespread standard for professional software development. The solution consists of three components that will be described in details in this chapter:

- The QKD Monitor software displays the values of the last minutes and last hours for each component (Alice, Bob, PolAlice, PolBob and QKD) in real-time.
- The QKD Control Client allows to change several of parameters on Alice and Bob like delays in real-time.
- The QKD Database is a MySQL database that holds every single value received by the QKD Monitor.

A.1. QKD Monitor

The QKD Monitor software (fig. A.1) receives, displays and logs data (measurement results and status messages) from all components used in the QKD system in real-time:

- From Alice: QBER, secure key rate, secure key size, sifted key size, number of wrong bits, number of disclosed bits during error correction, count rate of all four Si-detectors
- From Bob: coincidence rates of all four InGaAs-detectors
- From PolAlice: Coordinates of all six piezo channels, temperature of the crystal controller
- From PolBob: stokes parameters for the H and P reference pulse, distance to the target state before the PolCtrl cycle, distance after the PolCtrl cycle

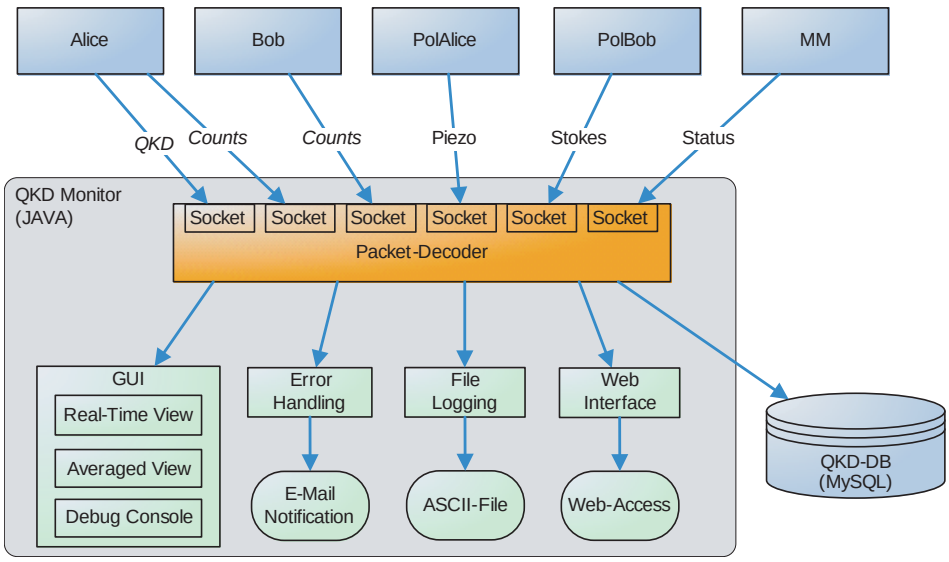

Figure A.1.: Basic scheme for the QKD Monitor software written in Java. Every component of the QKD system sends the data to the software where the packets are decoded. All values are displayed and logged to the QKD Database (optionally also to an ASCII file). One can choose between a real-time view of the latest values (∼15min) or a view with average values (several hours). Status messages from PolAlice and PolBob can be displayed on a "debug console". An internal interfaces allows to send error messages (e.g. detector failures) and periodic summaries via e-mail. Another interface allows to access the status of the QKD system over the internet via a (password secured) website.

Figure A.2.: Screenshot of the QKD Monitor showing data during the SECOQC conference. One can switch between the components (QKD, Alice, Bob, PolAlice, PolBob) using the tabs on the top. The data of the last 15 minutes or the last 2 hours is displayed in the main graph. The status line on the bottom gives some information on the duration and the database session.

Together with a remote-access software (e.g. TeamViewer [55]), we are able to view the status of the QKD system from anywhere via the internet. This has been an important feature during the SECOQC demonstration where Alice and Bob were located in different locations in Vienna.

A.2. QKD Control Client

This client was conceived to control the QKD process and some parameters on Alice and Bob during the laboratory tests. It has already been mentioned in section 6.4.1. The client allows to:

- Start and stop QKD
- Set the sifted key size
- Set the individual delay lines for Alice and Bob (see section 6.4.1)
- Set the auxiliary coincidence windows (see section 6.4.2) automatically or manually

Note that all of its functions have now been replaced by completely automated versions (FindDelay, FindWindow).

A.3. QKD Database

Because of the large amount of different type of data (count rates from Alice and Bob, status information from PolAlice and PolBob and QKD data) we have set up a MySQL database to manage the data. Databases are very commonly used for software development projects but rather not widespread for logging scientific data. Compared to the standard way of logging measurement results using text-based files, a database offers tremendous advantages. A professional planned database allows a structured storage of data, in our case measurement results. At the moment, the QDK Database holds about 150 million entries. Note that those entries are not single-photon measurements but mainly averaged (one second) values (count rates etc.). The Structured Query Language (SQL) allows reading, writing or deleting data using a vast amount of functions in a very convenient way. For a database containing scientific measurements, SQL is especially advantageous for the post-measurement analysis of the data.

The QKD database consists of six tables:

Table Session Contains basic information about a session which corresponds e.g. to a single measurement or a long-term QKD test		
Column	Data type	Comment
ID (PK)	Integer	Primary Key. Unique number that identifies a session with a numeric index. When starting a new measurements (session), the ID is incremented.
Name	Varchar	A short name that describes the session
StartTime	Datetime	Date and time when the session was started
EndTime	Datetime	Date and time when the session was stopped
Comment	Varchar	Some comments on the measurement, e.g. details on the environment

Table QKD Contains information on a block of secure key that leaves the QKD stack		
Column	Data type	Comment
SessionID (FK)	Integer	Foreign Key to the session
Number (PK)	Integer	A index that is incremented for every new row. It is set to one when a new session is started. SessionID and Number uniquely identify a measurement value
InsertTime	Datetime	Date and time when the values was added to the database
Block	Int	Block number
SysTime	Int	FPGA timestamp
QBER	Float	QBER in the block
Keysize	Int	Size of the secure key
SiftedKeysize	Int	Size of the sifted key
Keyrate	Float	Secure key rate of the block
DisclosedBits	Int	Number of disclosed bits during error correction

Table Alice Contains information on the count rates of Alice's detectors		
Column	Data type	Comment
SessionID (FK)	Integer	Foreign Key to the session
Number (PK)	Integer	Numeric index indicating the row
InsertTime	Datetime	Date and time when the values was added to the database
CountrateV	Float	Count rate of the vertical detector (one-second average)
CountrateH	Float	Count rate of the horizontal detector
CountrateP	Float	Count rate of the +45° detector
CountrateM	Float	Count rate of the -45° detector

Table Bob Contains information on the coincidence rates of Bob's detectors		
Column	Data type	Comment
SessionID (FK)	Integer	Foreign Key to the session
Number (PK)	Integer	Numeric index indicating the row
InsertTime	Datetime	Date and time when the values was added to the database
CountrateV	Float	Count rate of the vertical detector (one-second average)
CountrateH	Float	Count rate of the horizontal detector
CountrateP	Float	Count rate of the +45° detector
CountrateM	Float	Count rate of the -45° detector

Table PolAlice Contains status information of PolAlice (mainly SourceStab)		
Column	Data type	Comment
SessionID (FK)	Integer	Foreign Key to the session
Number (PK)	Integer	Numeric index indicating the row
InsertTime	Datetime	Date and time when the values was added to the database
MirrorX	Integer	Coordinate of the first axis of the mirror-piezo
MirrorY	Integer	Coordinate of the second axis of the mirror-piezo
Coupler810X	Integer	Coordinate of the first axis of the 810nm coupler-piezo
Coupler810Y	Integer	Coordinate of the second axis of the 810nm coupler-piezo
Coupler1550nmX	Integer	Coordinate of the first axis of the 1550nm coupler-piezo
Coupler1550nmY	Integer	Coordinate of the second axis of the 1550nm coupler-piezo
Temp	Float	Temperature of the non-linear crystals that produces the entangled photons

Table PolBob Contains status information of PolBob (mainly PolCtrl)		
Column	Data type	Comment
SessionID (FK)	Integer	Foreign Key to the session
Number (PK)	Integer	Numeric index indicating the row
StokesParam_HS_1	Float	initial Stokes parameter S1 for the H-pulse
StokesParam_HS_2	Float	initial Stokes parameter S2 for the H-pulse
StokesParam_HS_3	Float	initial Stokes parameter S3 for the H-pulse
StokesParam_PS_1	Float	initial Stokes parameter S1 for the P-pulse
StokesParam_PS_2	Float	initial Stokes parameter S2 for the P-pulse
StokesParam_PS_3	Float	initial Stokes parameter S3 for the P-pulse
ADC_H_1	Float	ADC value of polarimeter channel 1 (h-detector) for the H-pulse
ADC_H_2	Float	ADC value of polarimeter channel 2 (v-detector) for the H-pulse
ADC_H_3	Float	ADC value of polarimeter channel 3 (p-detector) for the H-pulse
ADC_H_4	Float	ADC value of polarimeter channel 4 (m-detector) for the H-pulse
ADC_H_5	Float	ADC value of polarimeter channel 5 (r-detector) for the H-pulse
ADC_H_6	Float	ADC value of polarimeter channel 6 (l-detector) for the H-pulse
ADC_P_1	Float	ADC value of polarimeter channel 1 (h-detector) for the P-pulse
ADC_P_2	Float	ADC value of polarimeter channel 2 (v-detector) for the P-pulse
ADC_P_3	Float	ADC value of polarimeter channel 3 (p-detector) for the P-pulse
ADC_P_4	Float	ADC value of polarimeter channel 4 (m-detector) for the P-pulse
ADC_P_5	Float	ADC value of polarimeter channel 5 (r-detector) for the P-pulse
ADC_P_6	Float	ADC value of polarimeter channel 6 (l-detector) for the P-pulse
Distance_Begin	Float	Distance to the target state before the PolCtrl cycle
Distance_End	Float	Distance to the target state after the PolCtrl cycle

B. Classical Description of Polarisation

This chapter will give a short overview of the classical description of polarisation as it is used for the polarisation stabilisation module (PolCtrl, see section 6.3). PolCtrl relies on strong reference pulses that have a known polarisation when the pulses enter the quantum channel. PolBob uses a polarimeter to measure the polarisation of the reference pulses after transmission. In contrast to the single photons, the polarisation of a classical wave can be completely determined and is usually described using the so-called Stokes parameters. To determine the polarisation, PolBob measures the power of the horizontal (H), vertical (V), +45 ° (P), -45 °, right handed (R) and left handed (L) components. This allows calculating the Stokes parameters:

$$S_0 = P_H + P_V \tag{B.1}$$
$$S_1 = P_H - P_V \tag{B.2}$$
$$S_2 = P_P - P_M \tag{B.3}$$
$$S_3 = P_R - P_L \tag{B.4}$$

The four Stokes parameters are combined to the Stokes vector:

$$\vec{S} = \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} \tag{B.5}$$

Usually, the Stokes vector is normalised using S_0:

$$\vec{S}_{norm} = \frac{\vec{S}}{S_0} \tag{B.6}$$

horizontal (H)	vertical (V)	+45° (P)	-45° (M)	right-handed (R)	left-handed (L)
$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \\ -0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$

Table B.1.: Example for some Stokes vectors

The three components S_1, S_2 and S_3 can be interpreted as coordinates that refer to a point on a unit-sphere called the Poincaré sphere (see for example figure 6.8).

In our case PolBob measures the analogue voltages of the detector that are proportional to the power. To obtain normalised Stokes parameters for the reference pulses as measured by PolBob, we have to consider the minimum voltage (no light) and maximum voltage (incident light is polarised identical as the polarisation that corresponds to the detector):

$$S_1 = \frac{V_H - V_{H,min}}{V_{H,max} - V_{H,min}} - \frac{V_V - V_{V,min}}{V_{V,max} - V_{V,min}} \tag{B.7}$$

Where $V_{x,min}$ is the minimum, $V_{x,max}$ the maximum and V_x the measured voltage, here in the H/V basis.. The same is valid for S_2 and S_3 , in the P/M and R/L basis.

The degree of polarisation (DOP) is defined as

$$DOP = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0} \tag{B.8}$$

A fully polarised waves (e.g. from a laser) has a DOP of 1 while a completely depolarised wave (e.g. classical thermal light) has a DOP of 0.

C. Acknowledgments

I want to thank everyone who contributed to realise the QKD system and achieving the results which I have been proud to present in this thesis. There is no doubt that this would not have been possible without the outstanding efforts of the whole team. Especially the preparations for the SECOQC demonstration were a stressful time, lasting not infrequently until late at night.

First, I want to thank Hannes Hübel for all his support in the last year, for giving me the chance to realise my ideas, to relieve me from all the nasty organisational issues and correcting this thesis.

I also want to thank the rest of the quantum cryptography team at the University of Vienna, especially Mike Hentschel for his help integrating the system to the 19-inch cases.

I want to thank the ARC-team: Thomas Matyus for his help implementing the management module, Thomas Lorünser for his help preparing and integrating the QKD system to the SECOQC network, Roland Lieger for his help implementing the synchronisation modules, and Andreas Poppe for all the valuable discussion throughout the last year and organising the excellent conference in October.

I also want to thank my former Siemens team, especially Andreas Hofmann and Bernard Führer for giving me the possibility to flexibly choose my working times allowing me to manage and studying physics and working for Siemens. Of course, I also want to thank Siemens for providing the infrastructure for the network demonstration. Notably, my former office was two floors above one of the node-rooms.

Finally, I want to thank Anton Zeilinger for giving me the chance to work in his group and for the financial support while writing up this thesis.

D. Curriculum Vitae

Alexander Treiber

Birthday	22nd November 1983 in Oberndorf/Salzburg
Address	Carl-Appel-Straße 9, 1100 Wien, Austria
E-Mail	alexander.treiber@univie.ac.at

Academic career

since 2003	Studies in physics, University of Vienna (interrupted Oct. 2004-Oct.2005 due to compulsory civilian service) Oct. 2004: first part finished with distinction Nov. 2007: second part finished with distinction
June 2003	Matura with distinction Diploma thesis "Bluetooth im Einsatz in Embedded Systems"
1998 - 2003	Secondary Technical College in Salzburg (HTL)
1994 - 1998	Secondary School in Salzburg

Vocational career

since 2007	Tutor for the electronics course, faculty of physics, University of Vienna
2005 - 2008	Software developer, Siemens SIS PSE
2004 - 2005	Compulsory civilian service in a kindergarten in Vienna (Kinder in Wien)
2003 - 2004	IT administrator, Austrian Student's Union
2001, 2002, 2003, 2004	Internships as software developer, Siemens PSE (Program and System Engineering) Salzburg

E. Zusammenfassung

Diese Arbeit präsentiert das erste vollautomatische, kompakte und zuverlässige Quantenkryptographie (Quantum Key Distribution - QKD) System auf Basis von verschränkten Photonen. Das System ist für die Integration in Standard 19-Zoll-Schränke konzipiert und arbeitet mit einer Wellenlänge von 1550nm für den optimalen Einsatz in Standard-Glasfasern. Mehrere neu entwickelte Stabilisierungs- und Automatisierungsmodule (u.a. Stabilisierung der Verschränkungsquelle, Stabilisierung der Polarisation in der Glasfaser und präzise Detektor-Synchronisation) sorgen für eine zuverlässige Verteilung von verschränkten Photonen.

Das QKD System wurde in das europäische SECOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography) Quantenkryptographie-Netzwerk integriert und im Oktober 2008 im Glasfaser-Netz von Siemens in Wien präsentiert. Während der zweiwöchigen Demonstration mit einer zwischen zwei Siemens-Standorten verlegten Glasfaser (16km, 4dB) konnte eine durchschnittliche Verschränkungs-Visibility von 93% erreicht werden. Über den gesamten Zeitraum hatten 99,9% aller Messwerte eine Visibility über 90%.

Die hohe Qualität der Verschränkung ermöglicht die Implementierung des BBM92 Quantum Key Distribution Protokolls. Gemeinsam mit der SECOQC Infrastruktur ermöglicht dies die Integration eines praxistauglichen Quantenkryptographie-Systems. Während der zweiwöchigen Testphase konnte eine stabile Schlüsselerzeugungsrate von über 2000 bit/Sekunde mit einer QBER (Quantum Bit Error Rate) von 3.5% erreicht werden ohne manuell in das System eingreifen zu müssen. Im Labor konnte eine Übertragung bis zu 50km bei einer Schlüsselerzeugungsrate von 500 bit/Sekunde erzielt werden.

Die Ergebnisse zeigen, dass es möglich ist, verschränkte Photonen in einem typischen innerstädtischen Glasfasernetzwerk mit hoher Qualität zuverlässig zu verteilen und für die Quantenkryptographie zu nutzen.

Bibliography

[1] A. Treiber et al. "Fully automated entanglement-based quantum cryptography system for telecom fiber networks. NJP 11, 045013, 2009. 7

[2] www.secoqc.net. 7, 9, 65, 67, 70

[3] A. Poppe et al. Outline of the SECOQC Quantum-Key-Distribution Network in Vienna. arXiv.org:quant-ph/0804.0122. 7, 66

[4] M. Peev et al. The SECOQC quantum key distribution network in Vienna. NJP 11, 075001, 2009. 7

[5] D.Mermin C.H.Bennett, G.Brassard. Quantum cryptography without Bells theorem. Phys. Rev. Lett. 68 557, 1992. 9, 22

[6] Bernhard Schrenk. Polarisationsnachregelung über lange Glasfaserstrecken fr Quantenkryptographie. Master's thesis, TU Wien, 2007. 10, 40, 41, 45

[7] Thorben Kelling. Towards a HandsOff Plug&Play Quantum Key Distribution System with Entangled Photons for a Quantum Network. Master's thesis, University of Heidelberg, 2008. 10, 34, 38, 40, 41, 43, 45, 46, 82

[8] Daniele Ferrini. Active polarization stabilization of entanglement based QKD for deployment in a city fiber link. Master's thesis, University of Roma, 2008. 10, 40, 41, 45

[9] N. Gisin et al. Quantum Cryptography. arXiv:quant-ph/01011098. 11

[10] V. Scarani et al. A Framework for Practical Quantum Cryptography. arXiv:quant-ph/0802.4155, 2008. 11

[11] T. Jennewein et al. Quantum Cryptography with entangled photons. PRL Vol. 84, 2000. 11

[12] A. Poppe et al. Practical Quantum Key Distribution with Polarisation Entangled Photons. Opt. Express 12, 2004. 11

[13] W.K. Wootters and W.H. Zurek. A Single Quantum Cannot be Cloned. Nature 299 (1982). 12

[14] N. Rosen B. Podolksy and A. Einstein. Can quantum-mechanical description of physical reality be considered complete? Physical Review, 47:777780, 1935. 14

[15] J.S. Bell. On the Einstein Podolsky Rosen paradox. Physics, 1(3):195, published by Physics Publishing Co., 1964. 14

[16] G. Weihs et al. Violation of bells inequality under strict Einstein locality conditions. PRL, 81 1998. 14

[17] A. Shamir R. Rivest and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21, 1978. 15

[18] R. Alleaume et al. SECOQC White Paper on Quantum Key Distribution and Cryptography. available on www.secoqc.net or arXiv.org:quant-ph/0701168. 15, 16

[19] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio. J. Amer. Inst. Elect. Eng. 55, 1926. 15

[20] W. Diffie and M. E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, Vol. IT-22, 1976. 16

[21] A.Samir and E.Tromer. Factoring Large Number with the TWIRL Device. CRYPTO 2003. 17

[22] T. Kleinjung. . http://www.crypto-world.com/announcements/m1039.txt. 17

[23] P.W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. IEEE Symposium on Foundations of Computer Science, 1994. 17

[24] S. Wiesner. Conjugate coding. Sigact News, 15-1, 78-88, 1983. 17

[25] C. H. Bennett and G. Brassard. Quantum Cryptography: public key distribution and coin tossing. Proceedings of the International Conference on Computer Systems and Signal Processing, Bangalore, page 175, 1984. 17

[26] C.E. Shannon. A Mathematical Theory of Communication. The Bell System Technical Journal, Vol. 27, 1984. 19

[27] G. Brassard and L. Salvail. Secret key reconciliation by public discussion. Lecture Notes in Computer Science, 765, 1994. 19

[28] G. Brassard C.H. Bennet and J.M. Robert. Privavy amplification by public discussion. SIAM Journal of Computation, 17:210229, 1988. 20

[29] N. Luetkenhaus. Security against individual attacks for realistic quantum key distribution. Physical Review Letters A, 61, 2000. 20

[30] X. Ma et al. Quantum key distribution with entangled photon sources. arXiv:quant-ph/0703122. 20, 58

[31] M. Koashi and J. Preskill. Secure quantum key distribution with an uncharacterized source. Phys. Rev. Lett., Vol. 90, 2001. 20

[32] idQuantique, http://www.idquantique.com. 21

[33] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences, 22, 1981. 21

[34] A. Ekert. Quantum cryptography based on Bells theorem. Phys. Rev. Lett., 67(6):661, 1991. 22

[35] H. Huebel et al. High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber. Optics Express, Vol. 15, Issue 12, 2007. 23, 62

[36] http://www.generalphotonics.com/PCD-M02.htm. 26, 35

[37] T. Loruenser et al. Security Processor with Quantum Key Distribution. Proc. IEEE ASAP 2008 37, 2008. 26, 70

[38] A.Treiber. Management module for the entangled QKD system. (project-internal specification). 37, 53

[39] www.generalphotonics.com/pdf/FAQPolariteII.pdf. 47

[40] C. Elliott et al. Current Status of The darpa Quantum Network. arxiv:quant-ph/0503058, 2005. 65

[41] R. Van Meter et al. System Design for a Long-Line Quantum Repeater. arXiv.org:quant-ph/0705.4128v2. 65

[42] T. Chen et al. Field test of a practical secure communication network with decoy-state quantum cryptography. arXiv.org:quant-ph/0810.1264. 65

[43] http://quantum.ukzn.ac.za/quantum-city. 65

[44] M. Dianati and R. Alleaume. Architecture of the Secoqc Quantum Key Distribution network. arXiv:quant-ph/0610202v2. 65

[45] O. Maurhart et al. Network Protocols for the QKD network. Secoqc deliverable D-NET-03, Oct. 2005. 71, 78

[46] A. Acin et al. Device-independent security of quantum cryptography against collective attack. arXiv:quant-ph/0702152. 81

[47] A. Lamas-Linares and C. Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. arXiv.org/quant-ph:0704.3297v2. 84

[48] Y. Zhao. Quantum hacking: experimental demonstration of time-shift attack against practical quantum key distribution systems. arXiv.org/quant-ph:0704.3253v2. 85, 86

[49] V.Makarov. Exploiting saturation mode of passively-quenched APD to attack quantum cryptosystems. arXiv.org/quant-ph:0707.3987v1. 87

[50] Z. L.Yuan et al. High speed single photon detection in the near-infrared. arXiv.org:quant-ph/0707.4307, 2007. 88

[51] Z. L.Yuan et al. Gigahertz quantum key distribution with InGaAs avalanche photodiodes. arXiv.org:quant-ph/0805.3414, 2008. 88

[52] E. Diamanti et. al. 100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors. Opt. Express, 14, 2006. 88

[53] H. Takesue et al. Quantum key distribution over 40 dB channel loss using superconducting single-photon detectors. Nature Photonics 1, 2007. 88

[54] id200 operating guide. http://www.idquantique.com/products/files/id200-operating.pdf. 88

[55] http://www.teamviewer.com. 91